

SOPHOS



User manual

Sophos Anti-Virus 4.5 for Windows NT/95/98/Me

Document version 1.0



About this manual

This user manual explains how to use Sophos Anti-Virus for Windows, and how to configure

- virus scanning
- virus alerts
- disinfection
- logging
- updating.

The manual also provides help in resolving common problems.

For information on the installation and initial setup of Sophos Anti-Virus, see the Sophos Anti-Virus Enterprise Solutions startup guide.

Contents

About Sophos Anti-Virus.....	1
Sophos Anti-Virus window.....	1
Sophos Anti-Virus system tray icon.....	4
Immediate and scheduled scanning.....	5
Running an immediate scan.....	5
Scheduling a scan.....	7
Changing items for immediate scanning.....	9
Changing items scanned by a scheduled job.....	10
Setting times of a scheduled job.....	12
Changing scanning options.....	13
Setting up automatic disinfection.....	15
Configuring reports.....	17
Changing types of executable for scanning.....	18
Excluding files from scanning.....	20
Scanning memory (98/Me).....	21
On-screen log virus detected messages.....	21
Enabling or disabling display of progress bar.....	23
On-access scanning.....	24
Checking on-access scanning is active.....	24
Changing scanning options.....	24
Setting up automatic disinfection.....	26
Selecting what is scanned.....	28
Excluding items from scanning.....	31
Starting and stopping scanning (Windows NT).....	33
Disinfection.....	36
Setting up automatic disinfection.....	36
Eliminating viruses.....	36
Recovering from virus side-effects.....	36
Configuring alerts.....	38
Desktop messaging.....	38
Event logging (Windows NT).....	39
Network messaging (Windows NT).....	41
SMTP email alerts.....	42
Logging.....	45
Setting the log folder.....	45
Clearing the on-screen log.....	45
Administration options.....	47
Restoring defaults.....	47
Purging checksums for virus-free files.....	47

Administration options

Locking settings for immediate scans.....47

Updating.....49

Updating manually.....49

Setting up automatic updating.....50

Setting a source for updates.....51

Setting an alternative source for updates.....52

Scheduling updates.....54

Updating via a proxy.....55

Limiting the bandwidth used.....56

Logging updates.....57

Troubleshooting.....59

Updating fails.....59

Scanning runs slowly.....60

Scheduled scans do not run (95/98/Me).....61

Virus not disinfected.....61

Virus fragment reported.....61

Sophos Anti-Virus reports errors.....62

About Sophos Anti-Virus

Sophos Anti-Virus is software that detects viruses, worms and trojans on your computer or network. It can also disinfect infected items. In particular, it can

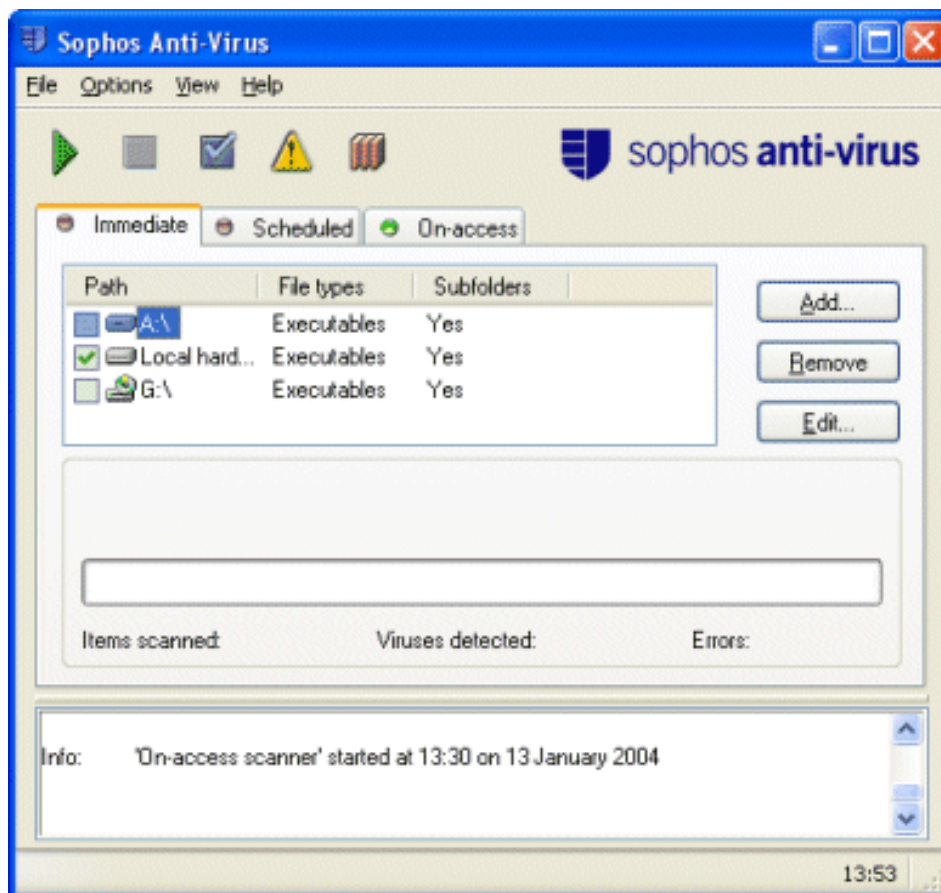
- scan your computer or network for viruses
- check each file you access for viruses
- eliminate viruses
- alert you when it finds a virus
- keep a log of its activity
- be updated to detect the latest viruses.

Sophos Anti-Virus consists of two main components:

- the **Sophos Anti-Virus** window
- the Sophos Anti-Virus system tray icon.

Sophos Anti-Virus window

To open the **Sophos Anti-Virus** window, at the taskbar, click **Start|Programs|Sophos|Sophos Anti-Virus|Sophos Anti-Virus**.



The components of the window are described in the following sections.

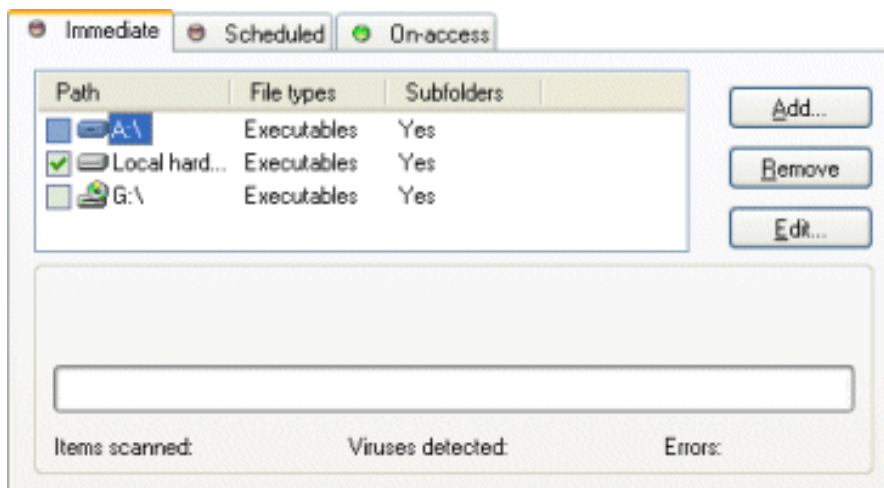
- Tabbed pages
- Button bar
- Scan list/job list
- On-screen log.

To close the **Sophos Anti-Virus** window, on the **File** menu, click **Exit**.

If Sophos Anti-Virus is running on Windows 95/98/Me, it may warn you that scheduled scans will not run if you close the window. This means if you want scheduled scans to run, the **Sophos Anti-Virus** window *must be open*.

Tabbed pages

In the **Sophos Anti-Virus** window, there is a tabbed page for each type of scan. Different tabs may be displayed. This depends on the version of Windows on the computer and the status of the user.



The tabs are as follows:

- **Immediate** for starting a scan at any time.
- **Scheduled** for scanning automatically at set times, as long as the computer is switched on.
- **On-access** for checking files when they are accessed.

Button bar

In the **Sophos Anti-Virus** window, the buttons are shortcuts to commonly-used menu options.

The button shown below starts scanning.



The button shown below stops scanning.



The button shown below opens a dialog box in which you can configure scanning.



The button shown below opens a dialog box in which you can configure virus alerts.



The button shown below connects you to virus analyses on the Sophos website.



Scan list/job list

In the **Sophos Anti-Virus** window, on the **Immediate** tabbed page, the scan list shows the drives, paths and files that can be scanned.

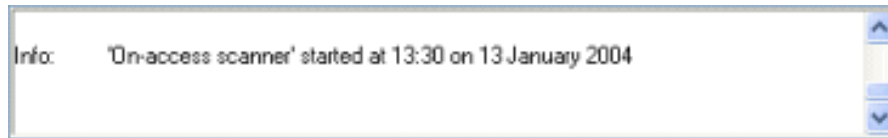
Path	File types	Subfolders
<input checked="" type="checkbox"/> Local hard drives	Executables	Yes
<input type="checkbox"/> G:\	Executables	Yes
<input checked="" type="checkbox"/> C:\Results.doc	N/A	Yes
<input checked="" type="checkbox"/> C:\del\	Executables	Yes

On the **Scheduled** tabbed page, the job list shows the currently active or inactive jobs.

Job Name	Days	Times
<input checked="" type="checkbox"/> Daily	Every day	21:00

On-screen log

In the **Sophos Anti-Virus** window, the on-screen log contains all messages logged since the window was opened.



On Windows 2000/XP/2003, if an Administrator user opens the **Sophos Anti-Virus** window, it also displays the scheduled and on-access messages logged since the service was started.

Sophos Anti-Virus system tray icon

The Sophos Anti-Virus system tray icon is always displayed, even if the **Sophos Anti-Virus** window is closed. While on-access scanning is active, the icon is blue.



If you pass the mouse over the icon, the hint displays the last time Sophos Anti-Virus was updated.

If you right-click the icon, a menu is displayed. From here, you can

- open the **Sophos Anti-Virus** window
- update Sophos Anti-Virus
- configure updating
- check the progress of an update.

Immediate and scheduled scanning

- ❓ An **immediate scan** is a virus scan of the computer, or parts of the computer, that you can carry out at any time.
- ❓ A **scheduled scan** is a scan of the computer, or parts of the computer, that takes place at a pre-specified time.

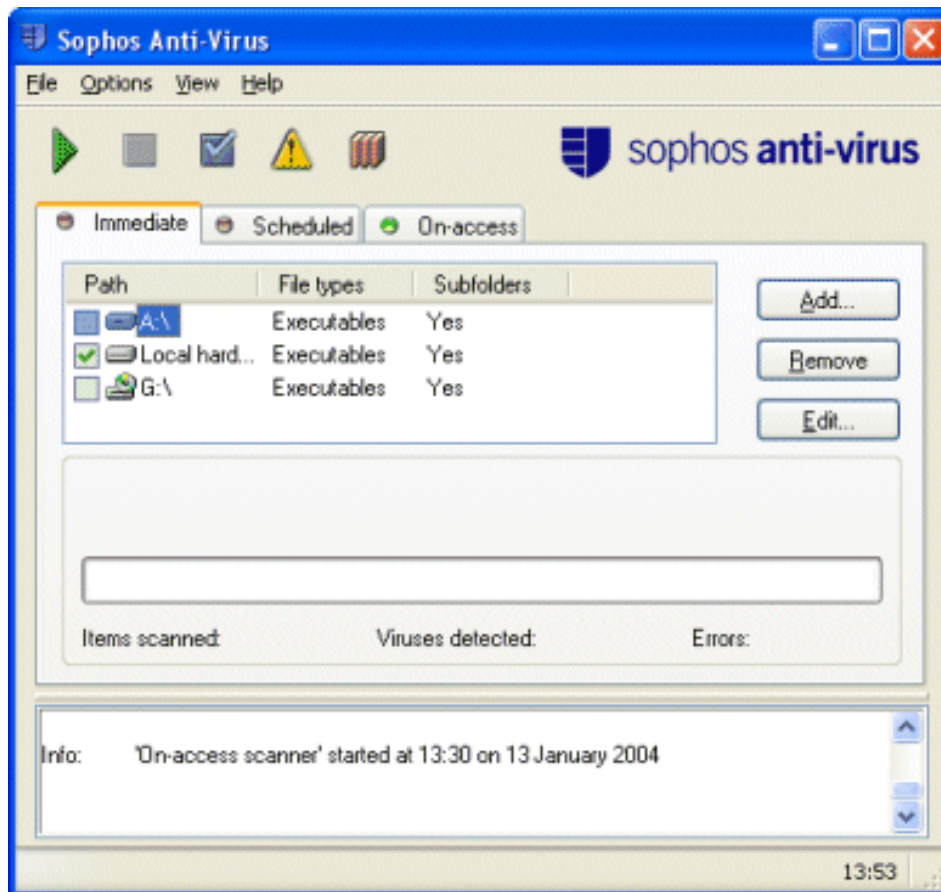
You can use Sophos Anti-Virus to

- run an immediate scan
- schedule a scan
- change items for immediate scanning
- change items scanned by a scheduled job
- set times of a scheduled job
- change scanning options
- set up automatic disinfection
- configure reports
- change types of executable for scanning
- exclude files from scanning
- scan memory (95/98/Me)
- view on-screen log virus detected messages
- enable or disable display of progress bar.

Running an immediate scan

- ❓ An **immediate scan** is a virus scan of the computer, or parts of the computer, that you can carry out at any time.

You run an immediate scan from the **Immediate** tabbed page of the **Sophos Anti-Virus** window.



The file list shows items that can be included in scans. A check box to the left of an item indicates whether it is activated and will be scanned. Click the check box to activate or deactivate items.

Starting an immediate scan

To scan all the selected items, click the button shown below.



Alternatively, on the **File** menu, click **Go**.

To scan any individual item in the file list, double-click its icon. (The check box to the left of the item doesn't have to be selected.)

Stopping an immediate scan

To stop scanning, click the button shown below.



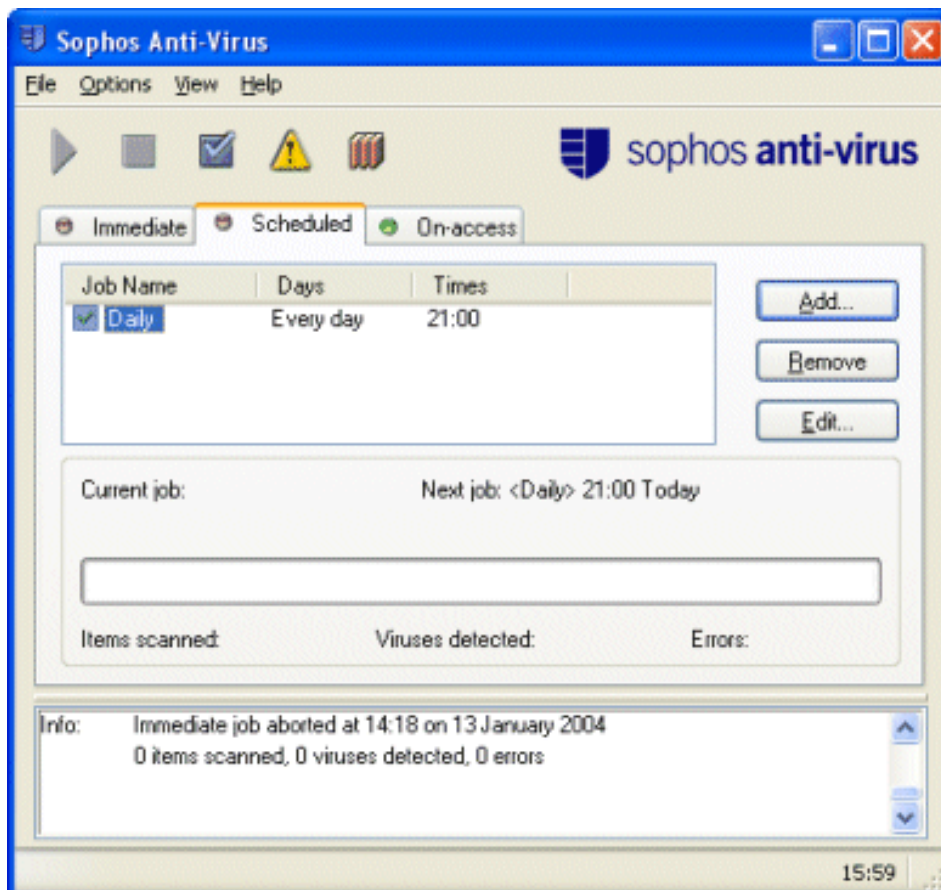
Alternatively, on the **File** menu, click **Stop**.

To add, remove or edit items for immediate scanning, see Changing items for immediate scanning.

Scheduling a scan

? A **scheduled scan** is a scan of the computer, or parts of the computer, that takes place at a pre-specified time.

You schedule a scan from the **Scheduled** tabbed page of the **Sophos Anti-Virus** window.



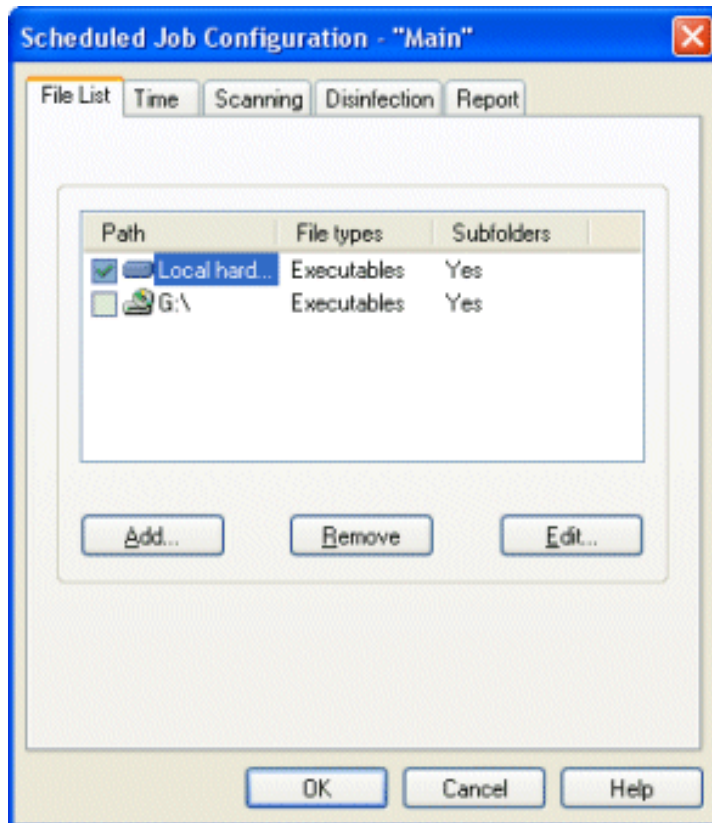
The job list shows the available scheduled scanning jobs. A check box to the left of a job indicates whether it is activated. An activated job will run, as long as the computer is switched on at the time and, if Sophos Anti-Virus is running on Windows 95/98/Me, the **Sophos Anti-Virus** window is open for the duration of the scan. Select the check box to activate or deactivate jobs.

On **Windows NT**, a default job called **Daily** scans the computer at 21.00 every day, as long as it is switched on at the time.

On **Windows 95/98/Me**, a default job called **Default** scans the computer at 13.00 every day, as long as it is switched on at the time and the **Sophos Anti-Virus** window is open for the duration of the scan.

Adding a scheduled job

In the **Scheduled** tabbed page, click **Add**. You are prompted to enter a job name. Type a name and click **OK** to display the **Scheduled Job Configuration** dialog box.



Use the **File List** and **Time** tabbed pages to specify what is scanned and when. For more information about configuring the job, see [Changing scanning options for immediate and scheduled scanning](#), [Setting up disinfection for immediate and scheduled scanning](#) and [Configuring reports](#).

Removing a scheduled job

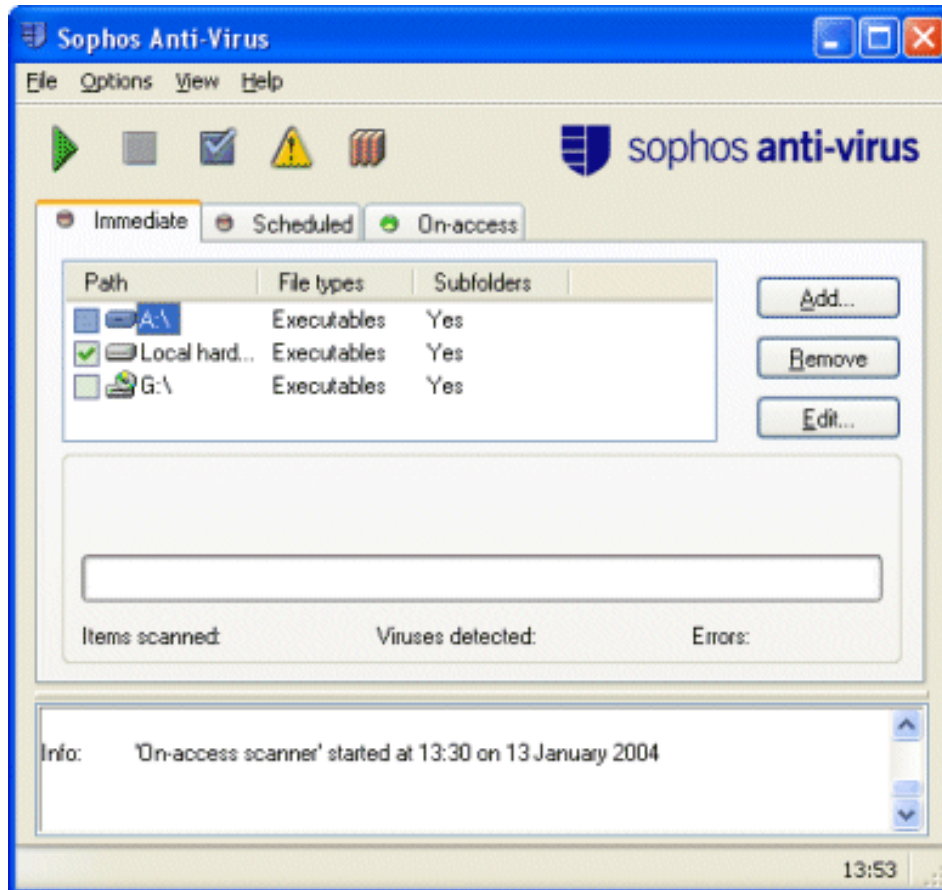
In the **Scheduled** tabbed page, select the name of the job you want to remove and click **Remove**.

Editing a scheduled job

In the **Scheduled** tabbed page, select the name of the job you want to edit and click **Edit** to display the **Scheduled Job Configuration** dialog box (shown above). Then configure the job as described in [Adding a scheduled job](#).

Changing items for immediate scanning

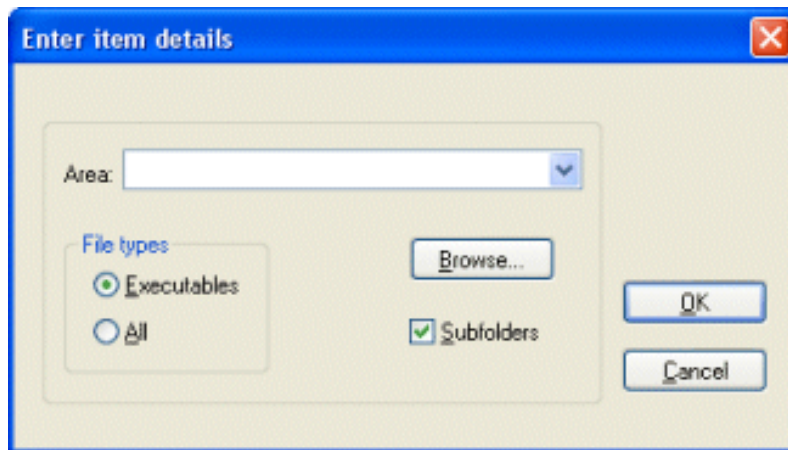
You change items for immediate scanning from the **Immediate** tabbed page of the **Sophos Anti-Virus** window.



By default, all local drives are included in the file list, and are activated for scanning. You can change the items in the file list as described below.

Adding an item for immediate scanning

In the **Immediate** tabbed page, click **Add** to display the **Enter item details** dialog box.



Area

Specify the drive, folder or file to be scanned. You can enter either mapped network drives or UNC path names. Alternatively, click **Browse** to select from available items, or use the drop-down list to select all **Local hard drives**.

File types

Only files defined as executables are scanned, unless you click **All**. See Changing types of executable for scanning to find out how to change the file types defined as executables.

Subfolders

If you select this option, subfolders are scanned.

Removing an item for immediate scanning

In the **Immediate** tabbed page, select the name of the item you want to remove and click **Remove**.

Editing an item for immediate scanning

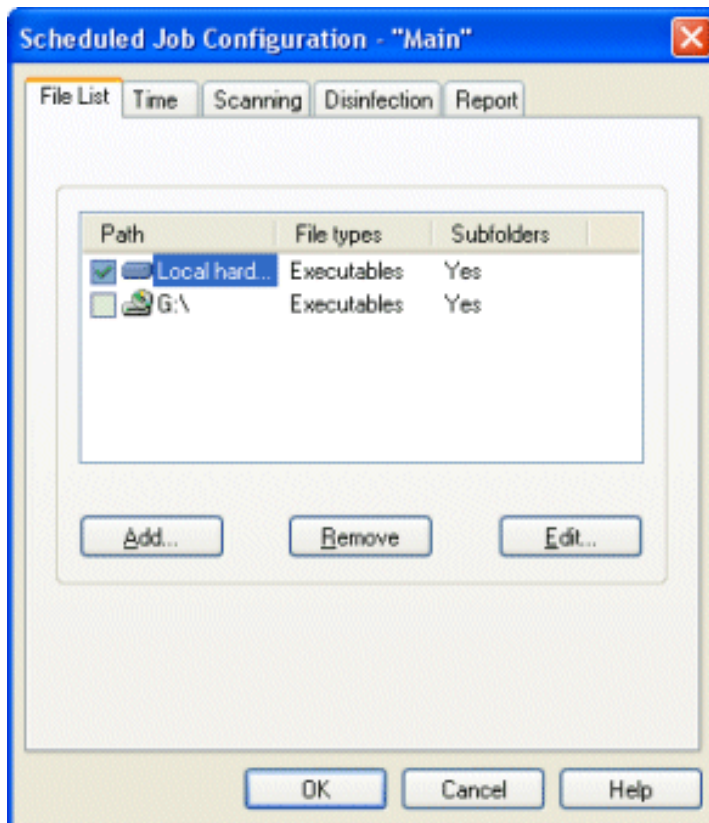
In the **Immediate** tabbed page, select the name of the item you want to edit and click **Edit** to display the **Enter item details** dialog box (described above).

Changing items scanned by a scheduled job

1. In the **Sophos Anti-Virus** window, click the **Scheduled** tab.
2. In the job list, select the scheduled job. Click the button shown below.




3. Click the **File List** tab.



A check box to the left of an item indicates whether it is activated and will be scanned. Click the check box to activate or deactivate items.

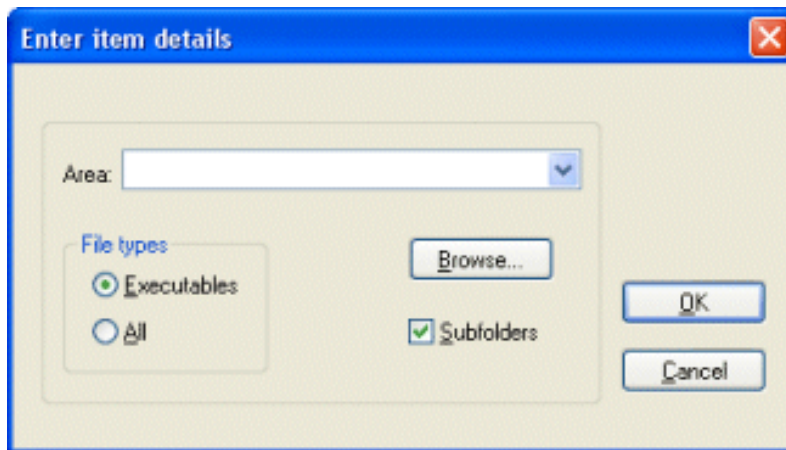
The default file list is the same as that for immediate scanning, except that local floppy disk drives are not listed.

 If Sophos Anti-Virus is running on Windows NT, the items available for scanning here might not be the same as those available for immediate scanning. This is because the scheduled scan runs with the Sophos Anti-Virus service's user rights, which may differ from those of the current user.

You can change the items in the file list as described below.

Adding an item for scheduled scanning

In the **File List** tabbed page, click **Add** to display the **Enter item details** dialog box.



Area

Specify the drive, folder or file to be scanned. You can enter either mapped network drives or UNC path names. Alternatively, click **Browse** to select from available items, or use the drop-down list to select all **Local hard drives**.

File types

Only files defined as executables are scanned, unless you click **All**. See Changing types of executable for scanning to find out how to change the file types defined as executables.

Subfolders

If you select this option, subfolders are scanned.

Removing an item for scheduled scanning

In the **File List** tabbed page, select the name of the item you want to remove and click **Remove**.

Editing an item for scheduled scanning

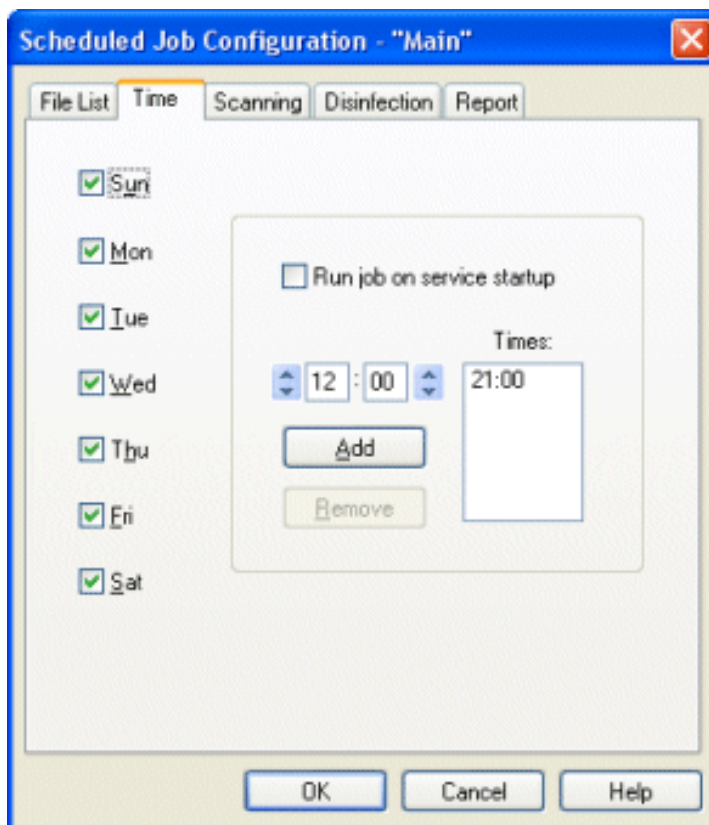
In the **File List** tabbed page, select the name of the item you want to edit and click **Edit** to display the **Enter item details** dialog box (described above).

Setting times of a scheduled job

1. In the **Sophos Anti-Virus** window, click the **Scheduled** tab.
2. In the job list, select the scheduled job. Click the button shown below.



3. Click the **Time** tab.



Select the day(s) on which the job should run. Then specify the time(s) as follows.

Add

To add a time, set the time and click **Add**.

Remove

To remove a time, select it and click **Remove**.

Run job on service startup (Windows NT only)

If you want this scheduled job to run whenever the Sophos Anti-Virus service is started, select this option. The scheduled job then takes place whenever the computer is booted and whenever Sophos Anti-Virus is updated.

Changing scanning options

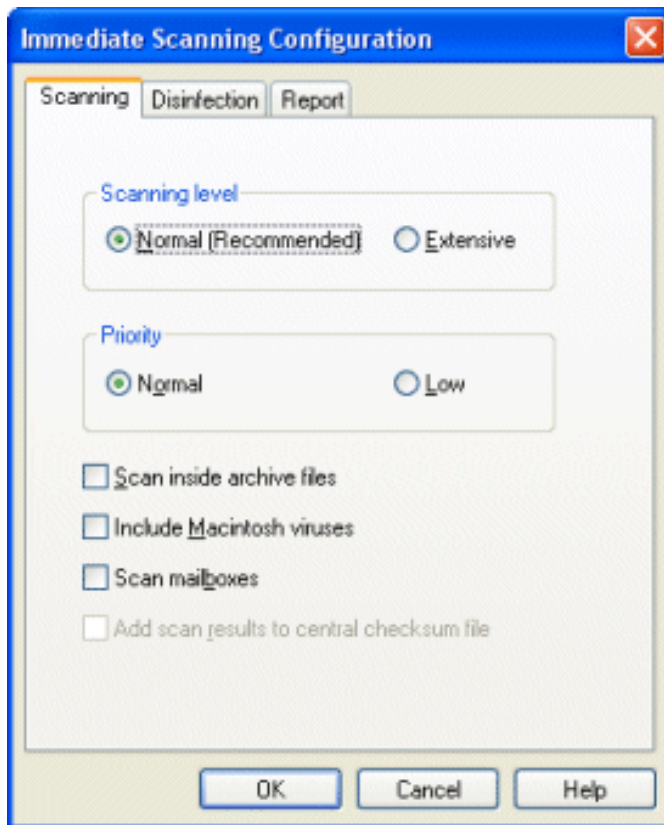
1. For **immediate** scanning, click the **Immediate** tab in the **Sophos Anti-Virus** window.

For **scheduled** scanning, click the **Scheduled** tab and select the scheduled job for which you want to change scanning options.

2. Click the button shown below.



3. Click the **Scanning** tab.



Scanning level

Normal scanning is sufficient for normal operation and scans those parts of each file that are likely to contain viruses.

Extensive scanning examines the complete contents of each file. This level is rarely required, would normally be used only on advice from Sophos technical support and is significantly slower than **Normal** scanning.

Priority

Set Sophos Anti-Virus to run at **Low** priority if you want to minimise the impact on system performance. Note that this increases the time Sophos Anti-Virus takes to perform a scan.

Scan inside archive files

If you want Sophos Anti-Virus to scan for viruses inside archive files, select this option. Archive types checked include: ARJ, BZIP2, CMZ, GZIP, InstallShield CAB, RAR, RAR3, RedHat Package Manager (RPM), Stuffit, TAR, Unix archive, ZIP. You can find a full list of archive types scanned in the Sophos Anti-Virus ReadMe.

- ❗ By default, files compressed with dynamic compression utilities (PKLite, LZEXE and Diet) are also scanned.
Even if you don't select this option, on-access scanning (see On-access scanning) still provides automatic protection from viruses
- ❗ in compressed files, because access to every unrecognised item (e.g. a newly decompressed file) is only granted after that item has been virus scanned.


Include Macintosh viruses (Windows NT only)

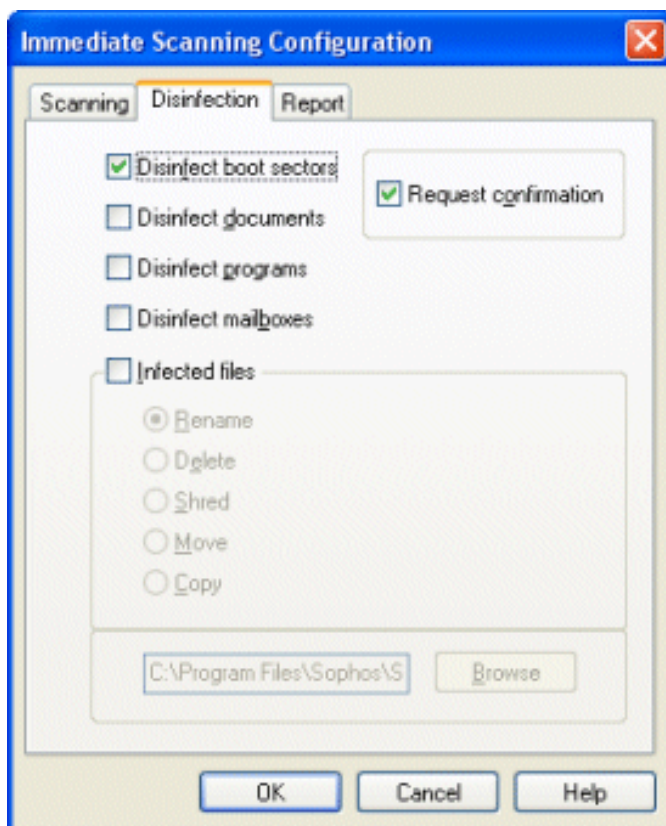
If you want Sophos Anti-Virus to scan for viruses inside Mac files, select this option. This enables Sophos Anti-Virus to scan executable Mac files, irrespective of their file extension.

Scan mailboxes

If you want Sophos Anti-Virus to scan emails and attachments in Outlook Express mailboxes, select this option.

Setting up automatic disinfection

1. For **immediate** scanning, click the **Immediate** tab in the **Sophos Anti-Virus** window.
For **scheduled** scanning, click the **Scheduled** tab and select the scheduled job for which you want to set up automatic disinfection.
2. Click the button shown below.

3. Click the **Disinfection** tab.



Disinfect boot sectors

Sophos Anti-Virus can disinfect most boot sector viruses on floppy disks. It does not automatically disinfect hard disk boot sectors. To deal with a virus in a hard disk boot sector, click the virus name in the on-screen log to view the virus analysis section of the Sophos website.

Disinfect documents

Sophos Anti-Virus can disinfect documents infected with most types of document virus. This removes the virus, but does not repair any changes the virus has made in the document (see the virus analysis section of the Sophos website for details of the virus's side-effects). If disinfection fails, the infected file is dealt with in the same way as other infected files (see **Infected files** below).

Disinfect programs

Sophos Anti-Virus can disinfect programs. Sophos recommends that you use this option only as a temporary measure. You should subsequently replace disinfected programs from the original disks or a clean backup.

Disinfect mailboxes

Sophos Anti-Virus can detect infected emails and attachments in Outlook Express mailboxes. All infected emails and attachments that can be disinfected, including those that are multiply-infected, are disinfected in one scan. At the end of the scan, Sophos Anti-Virus reports any emails or attachments that it could not disinfect.

Infected files

Sophos Anti-Virus can make an infected file safe in several ways other than disinfection.

Renaming or moving an executable file reduces the likelihood of it being run. Deleting or shredding the file disposes of it. Shredding is a more secure type of deletion that overwrites the contents of the file.

If you choose to move or copy files, you can select a folder for infected files from the browser.

The **Infected files** option does not apply to infected mailboxes.


Request confirmation

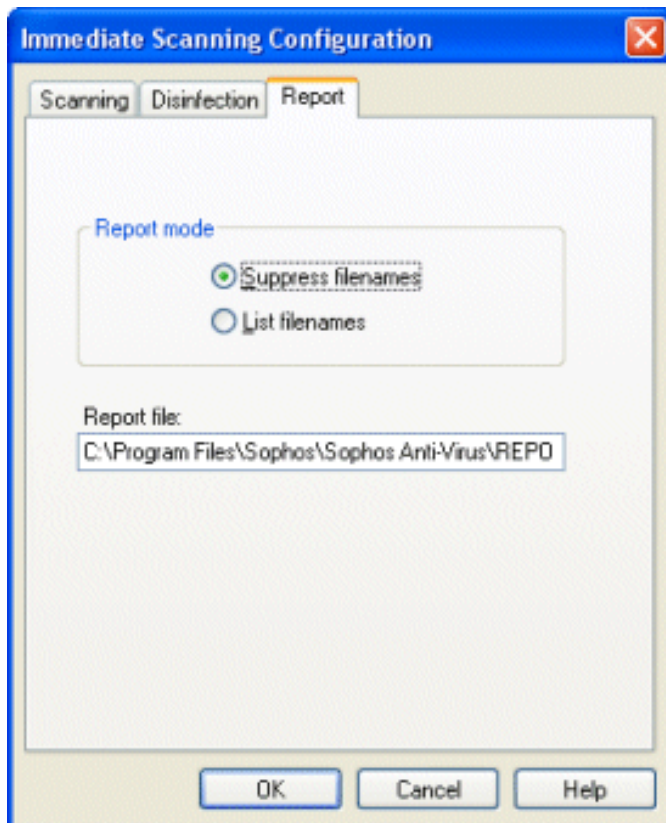
If you select this option, Sophos Anti-Virus asks for confirmation before it does anything that involves changing infected items (i.e. disinfecting, renaming, deleting, shredding or moving infected files).

! If you also select **Disinfect mailboxes**, Sophos Anti-Virus asks for confirmation only before disinfecting the *first* email or attachment it finds to be infected; it does *not* ask for confirmation before performing subsequent disinfections of the same mailbox in the same scan.

This option is only available for immediate scanning. It is selected by default.

Configuring reports

1. For **immediate** scanning, click the **Immediate** tab in the **Sophos Anti-Virus** window.
For **scheduled** scanning, click the **Scheduled** tab and then select the scheduled job for which you want to configure reports.
2. Click the button shown below.

3. Click the **Report** tab.



Sophos Anti-Virus generates a separate report file for each immediate or scheduled scan. This file is provided for the user. It is not the same as the continuous log file.

On Windows NT, the report file is written as the current user for immediate scans and as the service user for scheduled scans.

Report mode

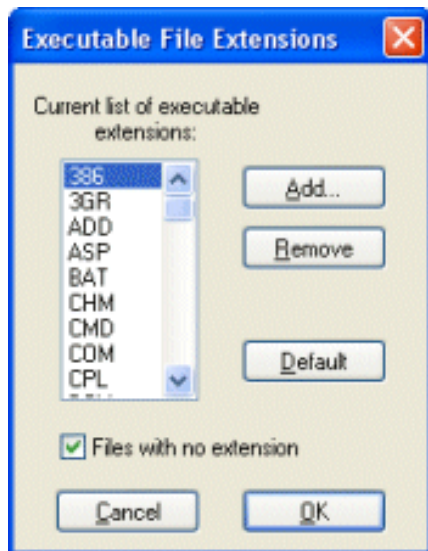
If you want Sophos Anti-Virus to record in the report file the name of every item scanned, click **List filenames**. Otherwise, accept the default.

Report file

Type a location for the report file or accept the default. This file is deleted and recreated for each immediate or scheduled scan.

Changing types of executable for scanning

To change the types of file that are scanned if Sophos Anti-Virus is set to scan only executables, on the **Options** menu, click **Executables**.



- To specify whether Sophos Anti-Virus scans **all** file types or only executables, see Changing items for immediate scanning or Changing items scanned by a scheduled job.

Adding an executable type

To add an executable type to the list, click **Add**. In the **New Executable Extension** dialog box, type the filename extension of the executable type.

Removing an executable type

To remove an executable type from the list, select the filename extension of the executable type you want to remove, and click **Remove**.

Selecting executables with no filename extension

To select executables whose filename has no extension, click **Files with no extension**.

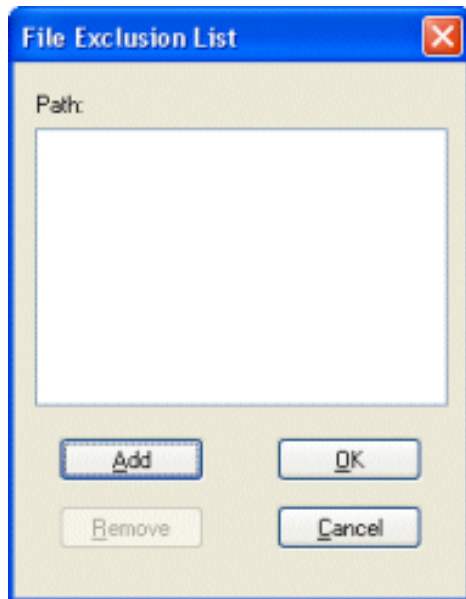
Using the default list of executable types

Unless you edit the list as explained above, it is automatically updated with filename extensions associated with new viruses, whenever you update Sophos Anti-Virus. If you want to discard your edits and revert to the default list (recommended), click **Default**.

On Windows NT, this dialog box is only available if you are logged on with Administrator rights.

Excluding files from scanning

On the **Options** menu, click **Exclusion List**.



All files listed are excluded from immediate and scheduled scanning. By default, they are also excluded from on-access scanning on Windows NT.

On Windows NT, this dialog box is only available if you are logged on with Administrator rights.

Adding a file

To add a file or filename extension to the list, click **Add**. In the **Exclude File** dialog box, enter the path of the file or the filename extension. To enter a filename extension, type eight question marks followed by the extension. For example, ????????.dta excludes all filenames ending in .dta from scanning, unless the filename is longer than eight characters. For filenames longer than eight characters, you must use the required number of question marks.



Using the asterisk wildcard character does not work in this dialog box.

Removing a file

To remove a file or filename extension from the list, select the file or filename extension you want to remove, and click **Remove**.

See also the section about excluding items from on-access scanning.

Scanning memory (95/98/Me)

To perform an immediate scan of memory, on the **File** menu, click **Scan memory**. This enables Sophos Anti-Virus to locate memory-resident viruses.

- Sophos Anti-Virus scans memory for memory-resident viruses automatically when it is first started.

On-screen log virus detected messages

The following messages can appear in the **Sophos Anti-Virus** window, in the on-screen log, when Sophos Anti-Virus detects a virus. They include the virus name, where the virus was found and the action taken. If you click a virus name, you can view the analysis of that virus on the Sophos website.

- In the descriptions below, text in square brackets indicates information that varies.

**Virus: [virus name] detected in [location]
[Action]**

This message is displayed if a virus is found during an immediate or scheduled scan. The [location] is one of

- [filename]
- Drive [drive name]:
- Sector [sector number]
- Disk [..]
- Cylinder [..]
- Head [..]
- Sector [..]
- Memory block at address [8 digit hex address]

The [action] taken depends on the disinfection settings. See Setting up automatic disinfection for immediate and scheduled scanning or Setting up automatic disinfection for on-access scanning. It is one of the following:

- No action taken
No action is taken if you have configured Sophos Anti-Virus not to disinfect, rename, delete, shred, move or copy any infected items.
- File deleted
The infected file has been deleted.
- File renamed to [filename]
The [filename] is the old name with the filename extension changed to a number. For example, if the infected file was named Virus.exe, it is renamed to Virus.000, or Virus.001 if there is already a file named Virus.000, and so on.

- File shredded
The infected file has been deleted and cannot be recovered.
- File moved to [new location]
The [new location] is the location specified in the disinfection settings.
- File copied to [new location]
The [new location] is the location specified in the disinfection settings.
- Error [problem]
The [problem] is one of the following: deleting [file], renaming to [file], shredding [file], moving to [file], copying to [file]. This means the file could not be deleted, renamed, shredded, moved or copied. If the infected file is on a floppy disk, check the disk is not write-protected.

❗ If the infected file is not deleted or shredded, it remains unchanged and may be able to infect other disks and files.

- Has been disinfected
Sophos Anti-Virus has automatically disinfected an item. Run an immediate scan to ensure the computer is now free of viruses (see Running an immediate scan).
- Error: Disinfection failed
Sophos Anti-Virus was unable to disinfect an item. See the Sophos website for information about disinfecting specific viruses.

❗ The infected item remains unchanged and may be able to infect other disks and files.

Virus fragment: [virus name] detected in [location]

No action taken

This message includes the name and location of the fragment. The [location] is one of the following:

- [filename]
- Drive [drive name]:
- Sector [sector number]
- Disk [..]
- Cylinder [..]
- Head [..]
- Sector [..]
- Memory block at address [8 digit hex address]

Sophos Anti-Virus does not remove virus fragments. See Virus fragment reported.

Enabling or disabling display of progress bar

You can choose whether or not the progress bar is displayed during an immediate or scheduled scan.

1. For **immediate** scanning, click the **Immediate** tab in the **Sophos Anti-Virus** window.
For **scheduled** scanning, click the **Scheduled** tab.
2. On the **View** menu, click **Progress Bar**.

This does not affect any scans already running.



To display the progress bar, Sophos Anti-Virus has to count the items to be scanned before starting. This can take a significant amount of time, which is saved by disabling the progress bar.

On-access scanning

? **On-access scanning** intercepts files as they are accessed, and grants access to only those that are virus free.

If your computer is on a network, or if your administrator has installed Sophos Anti-Virus for you, on-access scanning has probably already been configured. However, if you want to change the settings and your administrator has given you permission to change them permanently, you can do so.

On **Windows NT** computers, to change the settings for on-access scanning, use the **Sophos Anti-Virus** window. You must be logged in with local Administrator rights.

On **Windows 95/98/Me** computers, to change the settings for on-access scanning, edit the Interchk.cfg file in the installation folder (by default C:\Program Files\Sophos\Sophos Anti-Virus) using a text editor. Details of what you enter are given in the *InterCheck for Windows 95/98/Me advanced user guide*, available on the Sophos website.

With Sophos Anti-Virus, you can

- check on-access scanning is active
- change scanning options
- set up automatic disinfection
- select what is scanned
- exclude items from scanning
- start and stop scanning ((Windows NT)).

Checking on-access scanning is active

When on-access scanning is active, a blue shield is displayed in the system tray.



When on-access scanning is inactive, the shield is grey.

! Alternatively, on Windows NT, in the **Sophos Anti-Virus** window, click the **On-access** tab. The status is displayed here.

Changing scanning options

! The central console, if any, that administers Sophos Anti-Virus on workstations may override changes made here. To avoid this, see the console help.

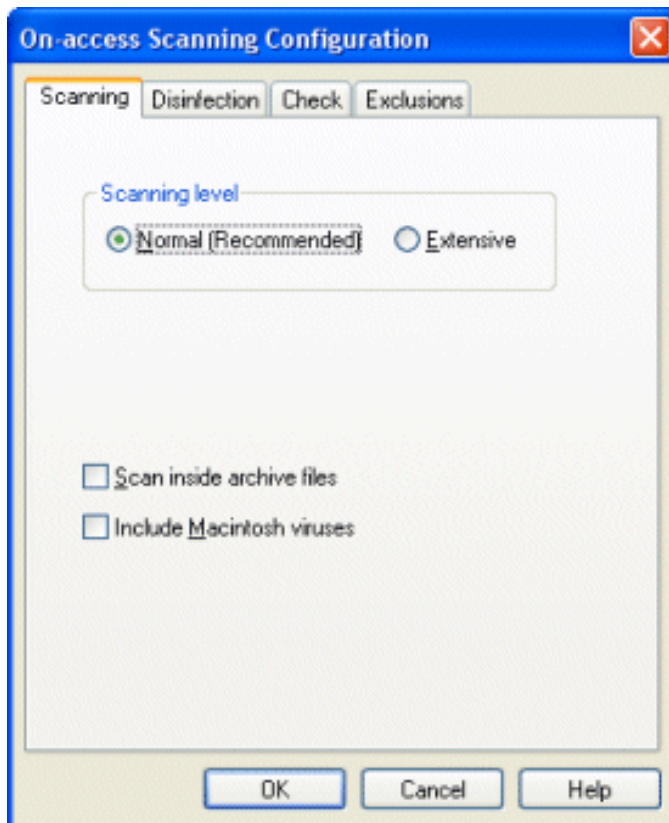
On **Windows 95/98/Me** computers, see On-access scanning.

On **Windows NT** computers, do as follows.

1. In the **Sophos Anti-Virus** window, click the **On-access** tab.
2. Click the button shown below.



3. Click the **Scanning** tab.



Scanning level

Normal scanning is sufficient for normal operation and scans those parts of each file that are likely to contain viruses.

Extensive scanning examines the complete contents of each file. This level is rarely required, would normally be used only on advice from Sophos technical support and is significantly slower than **Normal** scanning.

Scan inside archive files

If you want Sophos Anti-Virus to scan for viruses inside archive files, select this option. Archive types checked include: ARJ, BZIP2, CMZ, GZIP, InstallShield CAB, RAR, RAR3, RedHat Package Manager (RPM), Stuffit, TAR, Unix archive, ZIP. You can find a full list of archive types scanned in the Sophos Anti-Virus ReadMe.

- ❗ Whether you select this option or not, files compressed with dynamic compression utilities (PKLite, LZEXE and Diet) are scanned.
This option is rarely required and makes scanning significantly slower. Even if you don't select the option, on-access scanning still provides automatic protection from viruses in compressed files, because access to every unrecognised item (e.g. a newly decompressed file) is only granted after that item has been virus scanned.
- ❗

Include Macintosh viruses

If you want Sophos Anti-Virus to scan for viruses inside Mac files, select this option. This enables Sophos Anti-Virus to scan executable Mac files, irrespective of their file extension.

Setting up automatic disinfection


- ❗ The central console, if any, that administers Sophos Anti-Virus on workstations may override changes made here. To avoid this, see the console help.

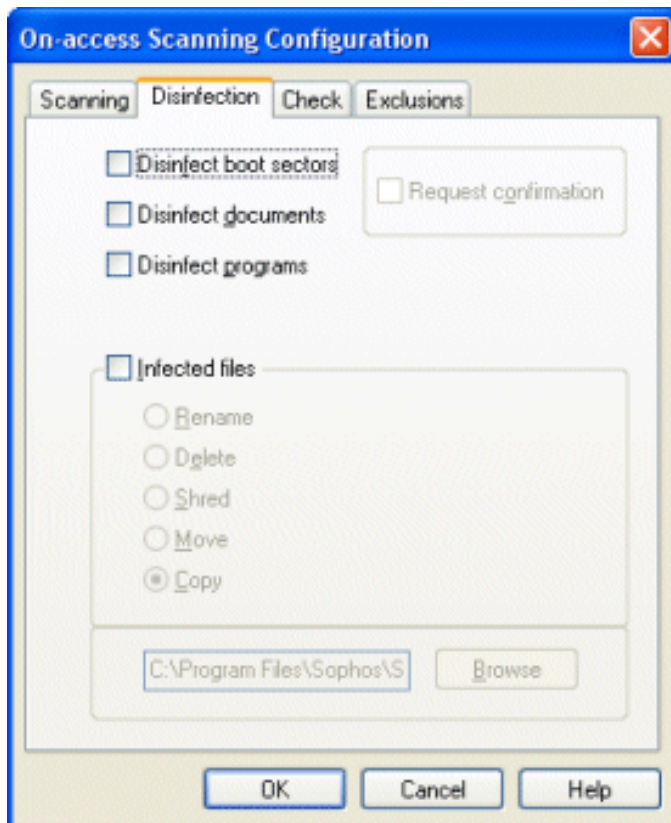
On **Windows 95/98/Me** computers, do as follows.

1. Edit the Interchk.cfg file in the installation folder (by default C:\Program Files\Sophos\Sophos Anti-Virus) using a text editor.
2. Type:
[SweepVxDWorkStation]
DisinfectDisks=YES
DisinfectDocuments=YES
3. Save and close the file.

For more information, see the *InterCheck for Windows 95/98/Me advanced user guide*, available on the Sophos website.

On **Windows NT** computers, do as follows.

1. In the **Sophos Anti-Virus** window, click the **On-access** tab.
2. Click the button shown below.

3. Click the **Disinfection** tab.



Disinfect boot sectors

Sophos Anti-Virus can disinfect most boot sector viruses on floppy disks. It does not automatically disinfect hard disk boot sectors. To deal with a virus in a hard disk boot sector, click the virus name in the on-screen log to view the virus analysis section of the Sophos website.

Disinfect documents

Sophos Anti-Virus can disinfect documents infected with most types of document virus. This removes the virus, but does not repair any changes the virus has made in the document (in the on-screen log, click the virus name to view details on the Sophos website of the virus's side-effects). If disinfection fails, the infected file is dealt with in the same way as other infected files (see **Infected files** below).

Disinfect programs

Sophos Anti-Virus can disinfect programs. Sophos recommends that you use this option only as a temporary measure. You should subsequently replace disinfected programs from the original disks or a clean backup.

Infected files

Sophos Anti-Virus can make an infected file safe in several ways other than disinfection.


Renaming or moving an executable file reduces the likelihood of it being run. Deleting or shredding the file disposes of it. Shredding is a more secure type of deletion that overwrites the contents of the file.

If you choose to move or copy files, you can select a folder for infected files from the browser.

The **Infected files** option does not apply to infected mailboxes.

Selecting what is scanned

You can select what is scanned by Sophos Anti-Virus and specify precisely **when** it is checked.

 The central console, if any, that administers Sophos Anti-Virus on workstations may override changes made here. To avoid this, see the console help.

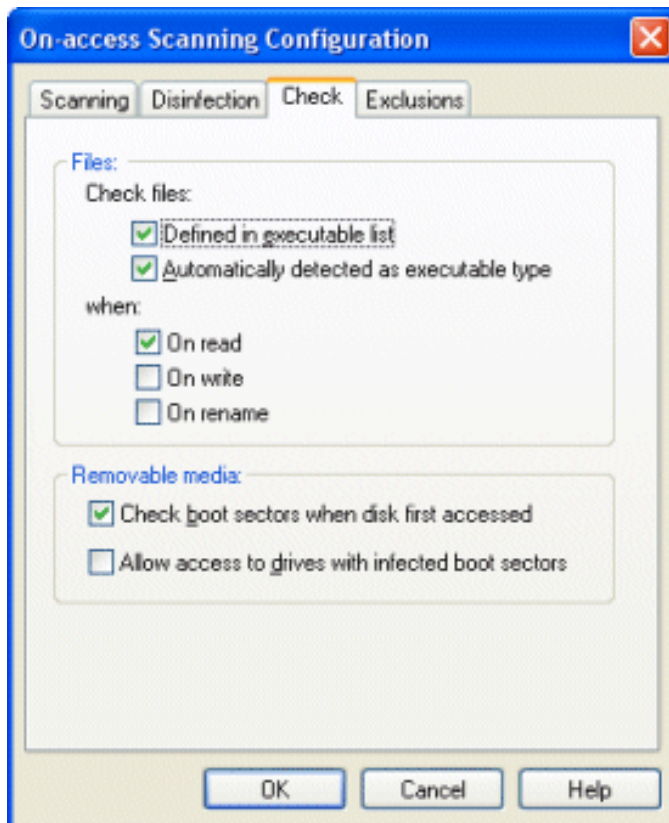
On **Windows 95/98/Me** computers, see On-access scanning.

On **Windows NT** computers, do as follows.

1. In the **Sophos Anti-Virus** window, click the **On-access** tab.
2. Click the button shown below.



3. Click the **Check** tab.



Check files

If you want Sophos Anti-Virus to check the file types specified in the executables list, select **Defined in executable list**. To change this list, see Changing types of executable for scanning.

If you want Sophos Anti-Virus to use file structure to determine whether to check files accessed, select **Automatically detected as executable type**. This option enables Sophos Anti-Virus to determine whether a file could potentially contain a virus.

You can select one or both of these options.

When

If you want Sophos Anti-Virus to check files when they are opened, select **On read**. By default, this option is selected.

If you want Sophos Anti-Virus to check files when they are closed, select **On write**.

If you want Sophos Anti-Virus to check files when they are renamed, select **On rename**.



These options give greater protection against viruses that write to the computer's hard drive and/or rename files. However, the increased activity may affect the computer's performance.

Removable media

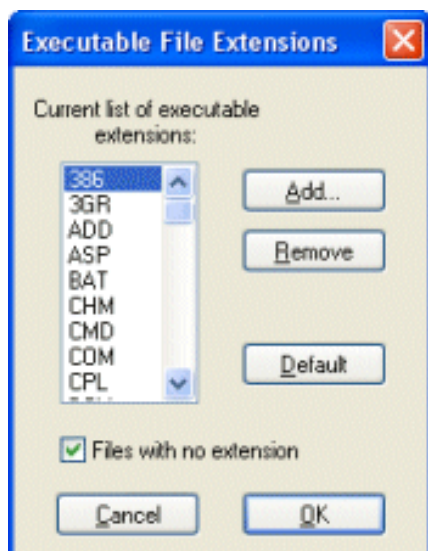
If you want Sophos Anti-Virus to check the boot sectors of all removable media when they are first used, select **Check boot sectors when disk first accessed**. By default, this option is selected.

If you want Sophos Anti-Virus to allow you to access drives that have infected boot sectors, select **Allow access to drives with infected boot sectors**. This option enables you to copy files from a floppy disk infected with a boot sector virus.

! Do not boot a computer from an infected disk. Doing so could infect the computer.

Changing types of executable for scanning

To change the types of file in the executables list, on the **Options** menu, click **Executables**.



On Windows NT, this dialog box is only available if you are logged on with Administrator rights.

Adding an executable type

To add an executable type to the list, click **Add**. In the **New Executable Extension** dialog box, type the filename extension of the executable type.

Removing an executable type

To remove an executable type from the list, select the filename extension of the executable type you want to remove, and click **Remove**.


Selecting executables with no filename extension

To select executables whose filename has no extension, click **Files with no extension**.

Using the default list of executable types

Unless you edit the list as explained above, it is automatically updated with filename extensions associated with new viruses, whenever you update Sophos Anti-Virus. If you want to discard your edits and revert to the default list (recommended), click **Default**.

Excluding items from scanning

 The central console, if any, that administers Sophos Anti-Virus on workstations may override changes made here. To avoid this, see the console help.

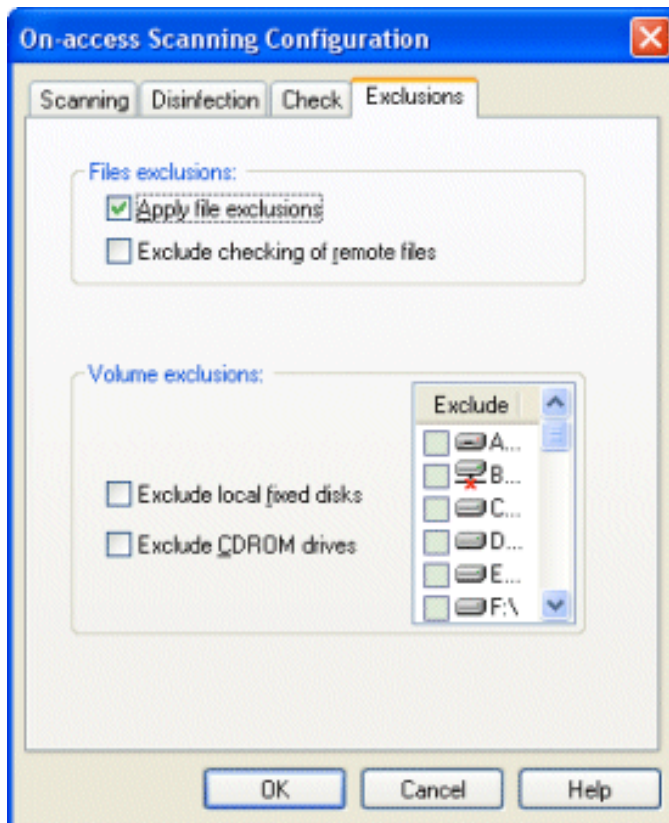
On **Windows 95/98/Me** computers, see On-access scanning.

On **Windows NT** computers, do as follows.

1. In the **Sophos Anti-Virus** window, click the **On-access** tab.
2. Click the button shown below.



3. Click the **Exclusions** tab.



File exclusions

If you want to prevent Sophos Anti-Virus from checking the file types specified in the exclusion list, select **Apply file exclusions**. To change this list, see Editing the list of files to be excluded.

If you want to prevent Sophos Anti-Virus from checking files on network drives, select **Exclude checking of remote files**.

Volume exclusions

Any drive(s) you select here are excluded from checking by Sophos Anti-Virus.

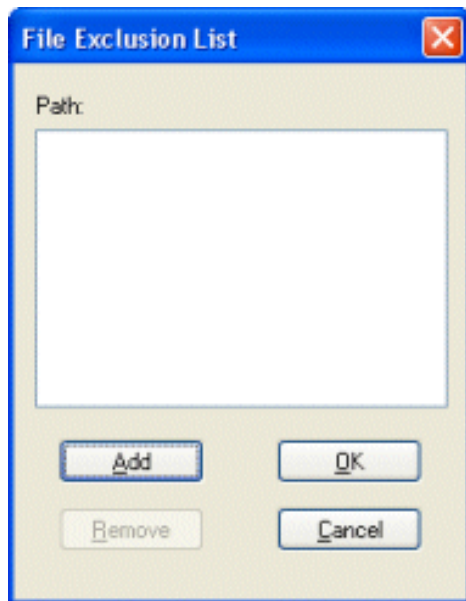
The **Exclude** list shows all possible drive mappings, whether or not the mapping is valid for a particular user. Drives that are unmapped for the current user are marked.

If you want to prevent Sophos Anti-Virus from checking all local fixed disks, whether or not they are specified in the **Exclude** list, select **Exclude local fixed disks**.

If you want to prevent Sophos Anti-Virus from checking all CD-ROM drives, whether or not they are specified in the **Exclude** list, select **Exclude CDROM drives**.

Editing the list of files to be excluded

On the **Options** menu, click **Exclusion List**.



All files listed are excluded from immediate and scheduled scanning. By default, they are also excluded from on-access scanning.

On Windows NT, this dialog box is only available if you are logged on with Administrator rights.

Adding a file

To add a file or filename extension to the list, click **Add**. In the **Exclude File** dialog box, enter the path of the file or the filename extension. To enter a filename extension, type eight question marks followed by the extension. For example, ???????.dta excludes all filenames ending in .dta from scanning, unless the filename is longer than eight characters. For filenames longer than eight characters, you must use the required number of question marks.



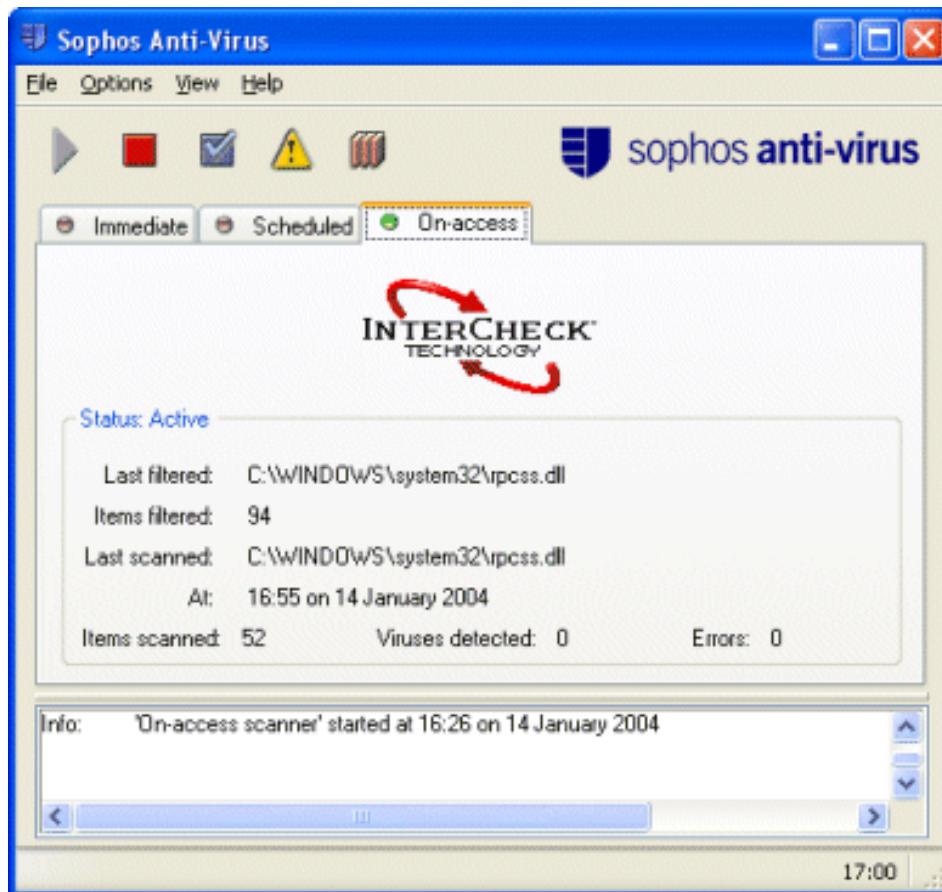
Using the asterisk wildcard character does not work in this dialog box.

Removing a file

To remove a file or filename extension from the list, select the file or filename extension you want to remove, and click **Remove**.

Starting and stopping scanning (Windows NT)

On Windows NT computers, you start or stop on-access scanning from the **On-access** tabbed page of the **Sophos Anti-Virus** window.



On-access scanning is active by default.

Starting on-access scanning

To start on-access scanning, click the button shown below.



Alternatively, on the **File** menu, click **Go**.

The shield that is displayed in the system tray turns blue.

Stopping on-access scanning

To stop on-access scanning, click the button shown below.



Alternatively, on the **File** menu, click **Stop**.

The shield that is displayed in the system tray turns grey.

- Sophos Anti-Virus retains the setting you make here, even after you reboot the computer. This means on-access scanning remains ***inactive*** until you start it again.

Disinfection

Sophos Anti-Virus can disinfect infected files or make them safe. You can:

- set up automatic disinfection
- eliminate viruses.

This section also tells you how to:

- recover from virus side-effects.

Setting up automatic disinfection


Sophos Anti-Virus can disinfect many infected files, or make them safe, automatically.

The procedure for setting up automatic disinfection depends on the type of scanning that you want to carry out the disinfection, and on the version of Windows you are using.

Click below for details of how to set up automatic disinfection for:

- immediate or scheduled scanning
- on-access scanning.

Eliminating viruses

 Sophos Anti-Virus can disinfect many viruses automatically. See the help pages on setting up automatic disinfection.

If a virus is found, Sophos Anti-Virus displays a virus warning. In the **Sophos Anti-Virus** window, in the on-screen log, click the virus name.



Sophos Anti-Virus connects you to the analysis of the virus on the Sophos website and advice on disinfection.

Recovering from virus side-effects

Recovery from virus infection depends on how the virus infected the computer. Some viruses leave you with no side-effects to deal with, others may have such

extreme side-effects that you have to restore a hard disk in order to recover.

Some viruses gradually make minor changes to data. This type of corruption can be hard to detect. It is therefore very important that you read the virus analysis on the Sophos website, and check documents carefully after disinfection.

Sound backups are crucial. You should keep original executables on write-protected disks so that infected programs can easily be replaced. If you did not have them before you were infected, create or obtain them in case of future infections.

Sometimes you can recover data from disks damaged by a virus. Sophos can supply utilities for repairing the damage caused by some viruses. Contact Sophos technical support for advice.

Configuring alerts


Sophos Anti-Virus can send alerts about viruses, errors and scanning activity.

You can set up:

- desktop messaging
- event logging (NT)
- network messaging (NT)
- SMTP email alerts.

By default, desktop messaging is enabled to send virus detected and error messages.

Desktop messaging

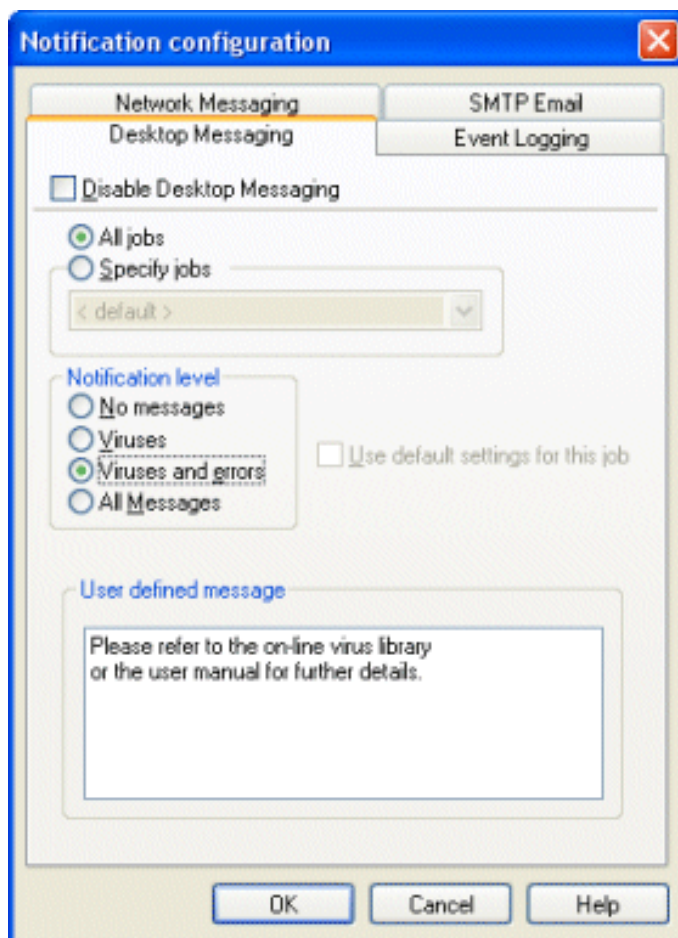
 The central console, if any, that administers Sophos Anti-Virus on workstations may override changes made here. To avoid this, see the console help.

To set up desktop messaging:

1. In the **Sophos Anti-Virus** window, click the button shown below.



2. Click the **Desktop Messaging** tab.
3. Deselect **Disable Desktop Messaging**.



Then set the options as described below.

Job specification

By default, alerts are sent for all scanning jobs. To specify settings separately for each job, select **Specify jobs**.

Notification level

If you want to change this, ensure that you deselect **Use default settings for this job**. Then set the types of event for which you want to receive alerts.

User defined message

Type a message that will be added to the end of the standard virus-detected message.

Event logging (Windows NT)

- ❗ The central console, if any, that administers Sophos Anti-Virus on workstations may override changes made here. To avoid this, see the

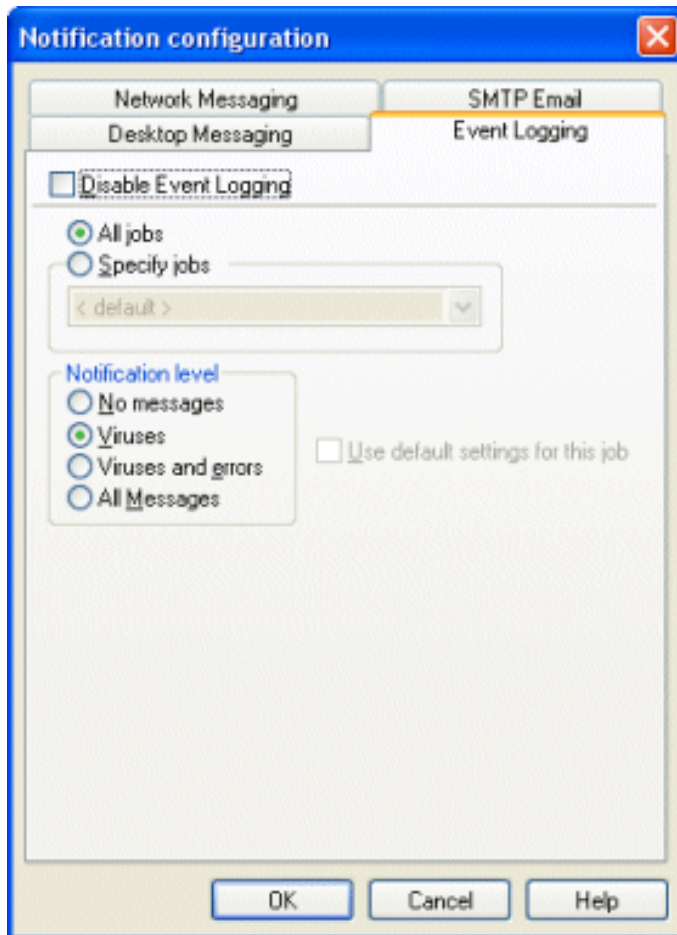
console help.

To specify the types of alert added to the Windows NT event log, do as follows. You must be an Administrator.

1. In the **Sophos Anti-Virus** window, click the button shown below.



2. Click the **Event Logging** tab.
3. Deselect **Disable Event Logging**.



Then set the options as described below.

Job specification

By default, alerts are sent for all scanning jobs. To specify settings separately for each job, select **Specify jobs**.

Notification level

If you want to change this, ensure that you deselect **Use default settings for this job**. Then set the types of event for which you want to receive alerts.

Network messaging (Windows NT)

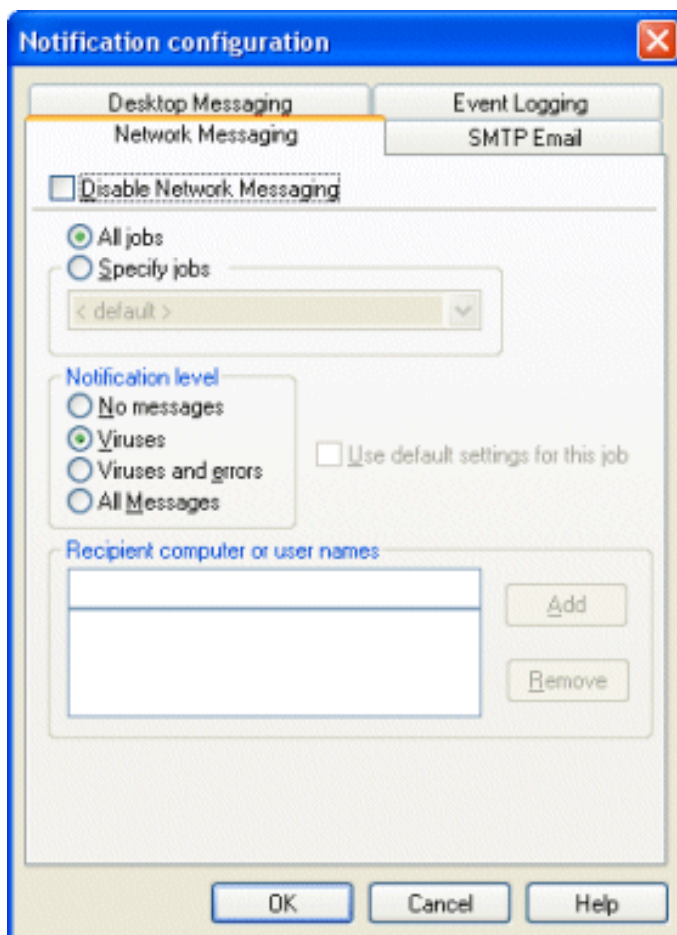
You can configure Sophos Anti-Virus to send network messages to named computers or users.

- ❗ The central console, if any, that administers Sophos Anti-Virus on workstations may override changes made here. To avoid this, see the console help.
- 💡 Due to limitations in the LAN Manager messaging system, only one message is delivered per name. Even if a username is logged onto several computers, only the first computer receives the message. Sophos therefore recommends that you enter computer names.
- 💡 Windows 95/98/Me computers can receive messages if they are running the WinPopUp application.

1. In the **Sophos Anti-Virus** window, click the button shown below.



2. Click the **Network Messaging** tab.
3. Deselect **Disable Network Messaging**.



Then set the options as described below.

Job specification

By default, alerts are sent for all scanning jobs. To specify settings separately for each job, select **Specify jobs**.

Notification level

If you want to change this, ensure that you deselect **Use default settings for this job**. Then set the types of event for which you want to receive alerts.

SMTP email alerts

You can configure Sophos to send email alerts. Mail is sent after each event encountered by on-access scanning, or at the end of an immediate or scheduled scan.

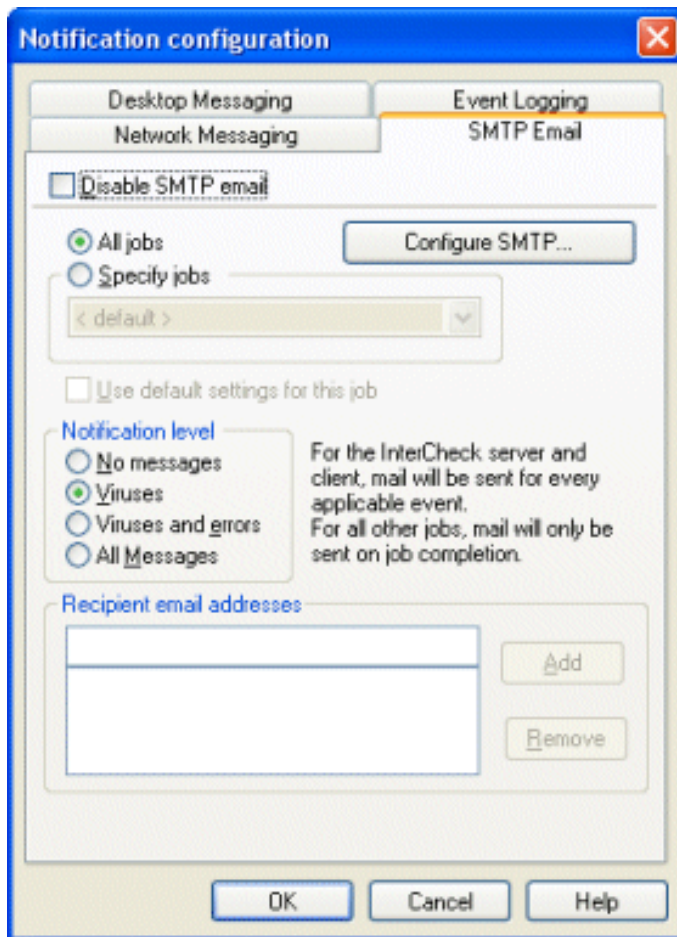


The central console, if any, that administers Sophos Anti-Virus on workstations may override changes made here. To avoid this, see the console help.

1. In the **Sophos Anti-Virus** window, click the button shown below.



2. Click the **SMTP email** tab.
3. Deselect **Disable SMTP email**.



Then set the options as described below.

Configure SMTP

Click this to enter details of the SMTP server. In the **Set up SMTP** dialog box, enter the host name or IP address of the SMTP server. In the same dialog box, in the **SMTP sender address** text box, enter an email address that bounces and non-delivery reports can be sent to.

Job specification

By default, alerts are sent for all scanning jobs. To specify settings separately for each job, select **Specify jobs**.

Notification level

If you want to change this, ensure that you deselect **Use default settings for this job**. Then set the types of event for which you want to receive alerts.

Recipient email addresses

Use the **Add** and **Remove** buttons to add or remove addresses for recipients of email alerts.

Logging

Sophos Anti-Virus logs its activity in two places.

- ? The **log file** is a continuous log file aimed at the administrator. On Windows NT, it is written as the Sophos Anti-Virus service user and not as the current user.
- ? The **on-screen log** is displayed at the bottom of the **Sophos Anti-Virus** window. It contains all messages logged since the window was opened. On Windows NT, if an Administrator user opens the **Sophos Anti-Virus** window, it also displays the scheduled and on-access messages logged since the service was started.

You can:

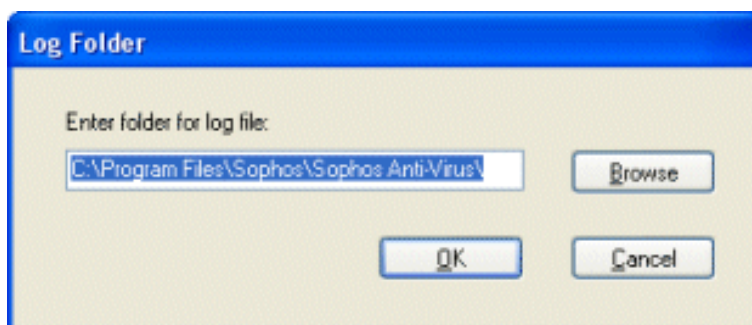
- change the location of the log file
- clear the on-screen log.

Setting the log folder

By default, Sophos Anti-Virus maintains a log file of all its activity in the Sophos Anti-Virus folder.

If you are logged on with Administrator rights, you can change the location of the log file:

1. On the **File** menu, click **Set Log Folder**.
2. In the **Log Folder** dialog box, specify a folder and click **OK**.



Clearing the on-screen log

The **on-screen log** is displayed at the bottom of the **Sophos Anti-Virus** window. It contains all messages logged since the window was opened. On Windows NT, if an Administrator user opens the **Sophos Anti-Virus** window, it also displays the scheduled and on-access messages logged since the service was started.

To clear the on-screen log, on the **Options** menu, click **Clear log**.



This does not affect the Sophos Anti-Virus log file.


Administration options

In Sophos Anti-Virus, you can:



- restore default settings
- purge the checksums for files already found to be virus-free
- lock the settings for immediate scans.

Restoring defaults

You can return all settings to their defaults.

 The central console, if any, that administers Sophos Anti-Virus on workstations may override changes made here. To avoid this, see the console help.

In the **Sophos Anti-Virus** window, on the **Options** menu, select **Restore Defaults**.


-  If you are not logged on with Administrator rights, you can only restore defaults for immediate scanning.
-  Restoring defaults deletes all scheduled jobs.

Purging checksums for virus-free files

Sophos Anti-Virus stores checksums for files that on-access scanning has already found to be free of viruses.

You can clear the checksums. The on-access scanner will then have to scan the files again the next time they are accessed.

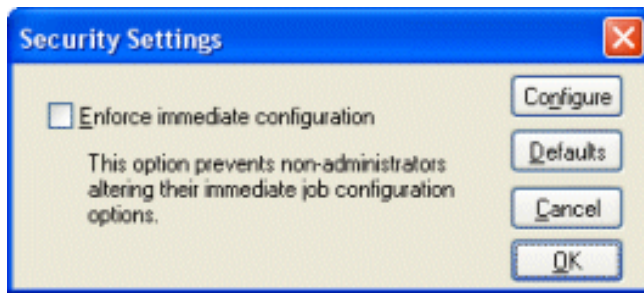
In the **Sophos Anti-Virus** window, on the **Options** menu, click **Purge Checksums**.

-  This option is only available if you are logged on with Administrator rights.

Locking settings for immediate scans

Administrators can configure an immediate scanning job that is then used by all non-Administrators.

1. In the **Sophos Anti-Virus** window, on the **Options** menu, click **Security**.
2. In the **Security settings** dialog box, configure the settings as described below.



Configure

When you click **Configure**, the **Admin Defined User Mode Configuration** dialog box is displayed. Select the configuration options for users' installations.

Defaults

This returns the options to their default settings.

Enforce immediate configuration

Select this if you want to prevent non-Administrator users from changing their immediate scanning configuration.

Updating

Sophos Anti-Virus must be updated regularly to enable it to detect all the latest viruses.


If your computer is on a network, or if your administrator has installed Sophos Anti-Virus for you, Sophos Anti-Virus has probably already been configured to update itself automatically.

If you need to set up automatic updating, or want to change the updating settings, you can do so. However, on Windows NT, you must be logged in with local Administrator rights.

This section describes how to:

- update manually
- set up automatic updating
- set a source for updates
- set an alternative source for updates
- schedule updates
- update via a proxy
- limit the bandwidth used
- log updates.

Updating manually


 If you have installed Sophos Anti-Virus as recommended in Sophos documentation, updating occurs automatically.

If you want to update Sophos Anti-Virus manually, you can do so.

1. Locate the Sophos Anti-Virus icon in the system tray (shown below).



2. Right-click and select **Update now**.

 Alternatively, double-click the Sophos Anti-Virus icon.

Provided Sophos Anti-Virus has been correctly configured, it checks the usual source for new software and, if necessary, updates itself.

For information on configuring updating, see the other pages in this section.

Setting up automatic updating

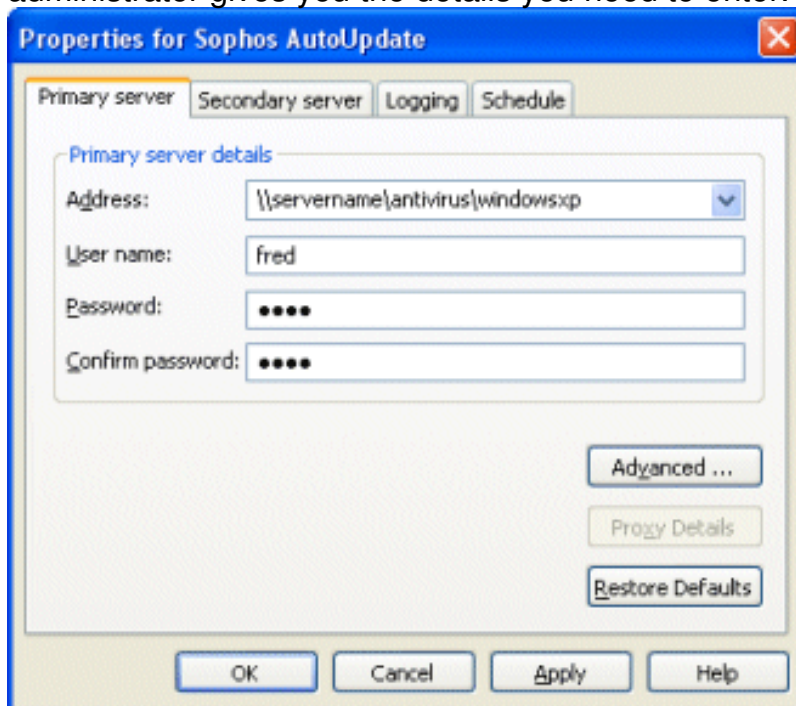
If your computer is on a network, or if your administrator installed Sophos Anti-Virus for you, Sophos Anti-Virus has usually been set to update itself automatically.

If automatic updating has not been set up, follow the steps below. For full information on the options at each step, see the section describing that configuration page.

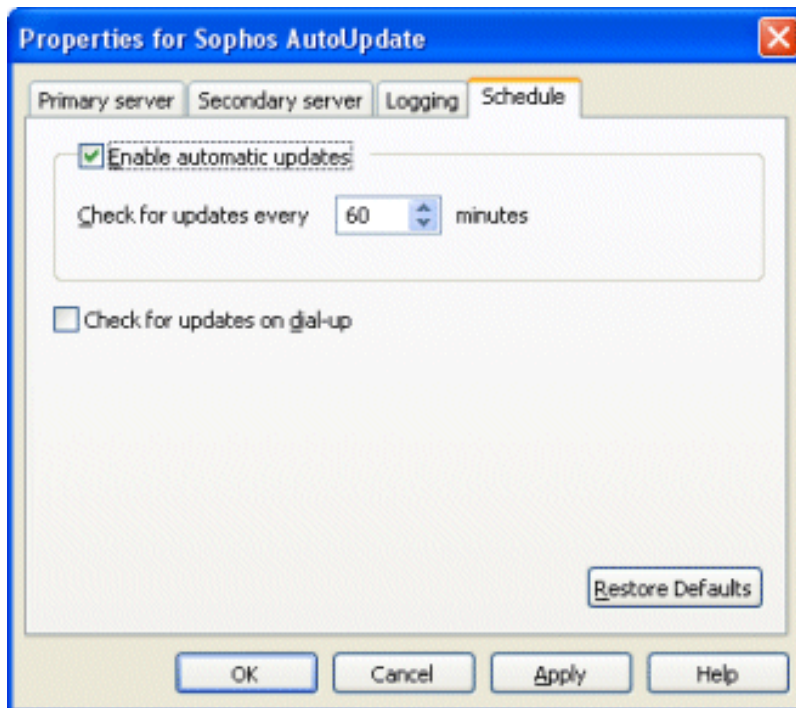
1. Locate the Sophos Anti-Virus icon in your system tray. Right-click it and select **Configure**.



2. Click the **Primary server** tab and set the source for updates. Your administrator gives you the details you need to enter.



3. Click the **Schedule** tab and schedule updates.



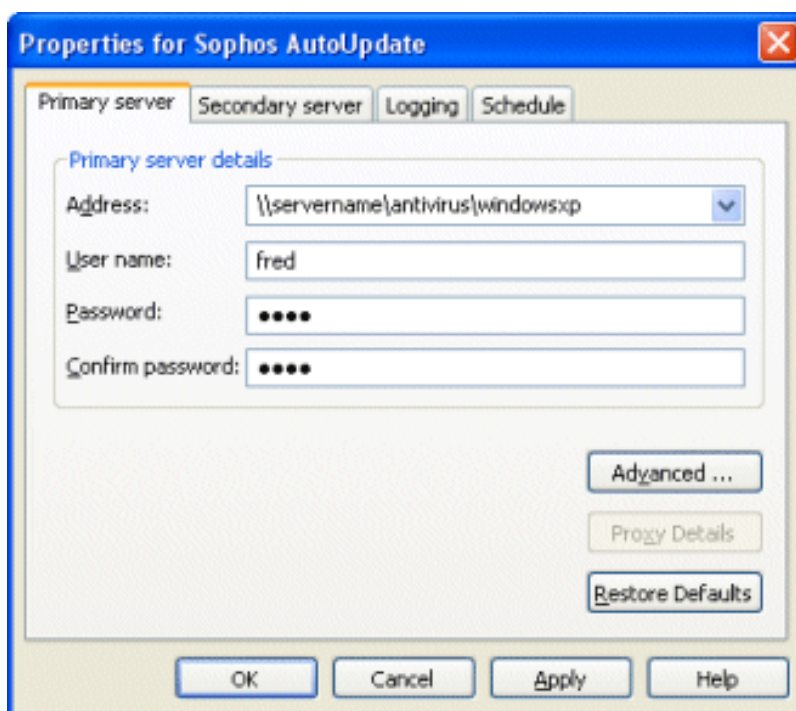
Setting a source for updates

If you want Sophos Anti-Virus to update itself automatically, you must specify where it fetches updates from.

1. Locate the Sophos Anti-Virus icon in your system tray. Right-click and select **Configure**.



2. Click the **Primary server** tab and enter the details needed as described below.



Address

Enter the address (UNC path or web address) from which Sophos Anti-Virus will usually fetch updates. If you select **Sophos**, Sophos Anti-Virus will download updates directly from Sophos via the internet.

- ❗ Your administrator supplies you with the address and account details you need.

User name

If necessary, enter the **User name** for the account that will be used to access the server, and then enter and confirm the **Password**.

- ❗ If the **User name** needs to be qualified to indicate the domain, use the form domain\username.

If you want to limit the bandwidth used, click **Advanced**.

If you access the internet via a proxy server, click **Apply** and then **Proxy Details**. Note that some internet service providers require web requests to be sent to a proxy server.

Setting an alternative source for updates

You can set an alternative source for updates. If Sophos Anti-Virus cannot contact its usual source, it will attempt to update from this alternative source.

1. Locate the Sophos Anti-Virus icon in your system tray. Right-click on it and select **Configure**.



2. Click the **Secondary server** tab. Then enter the details as described below.

The screenshot shows the 'Properties for Sophos AutoUpdate' dialog box with the 'Secondary server' tab selected. The 'Secondary server details' section contains four input fields: 'Address' (a dropdown menu showing 'http://www.mycompany.com/'), 'User name' (text box with 'fred'), 'Password' (password box with four dots), and 'Confirm password' (password box with four dots). To the right of these fields are three buttons: 'Advanced ...', 'Proxy Details', and 'Restore Defaults'. At the bottom of the dialog are four buttons: 'OK', 'Cancel', 'Apply', and 'Help'.

Address

Enter the **Address** (UNC path or web address) from which Sophos Anti-Virus will fetch updates if it cannot contact the usual source. If you select **Sophos**, Sophos Anti-Virus will download updates directly from Sophos via the internet.

- 💡 Your administrator supplies you with the address and account details you need.

User name

If necessary, enter the **User name** for the account that will be used to access the server, and then enter and confirm the **Password**.

- 💡 If the **User name** needs to be qualified to indicate the domain, use the form domain\username.

If you want to limit the bandwidth used, click **Advanced**.

If you access the address via a proxy server, click **Apply** and then **Proxy Details**. Note that some internet service providers require web requests to be sent to a proxy server.

Scheduling updates

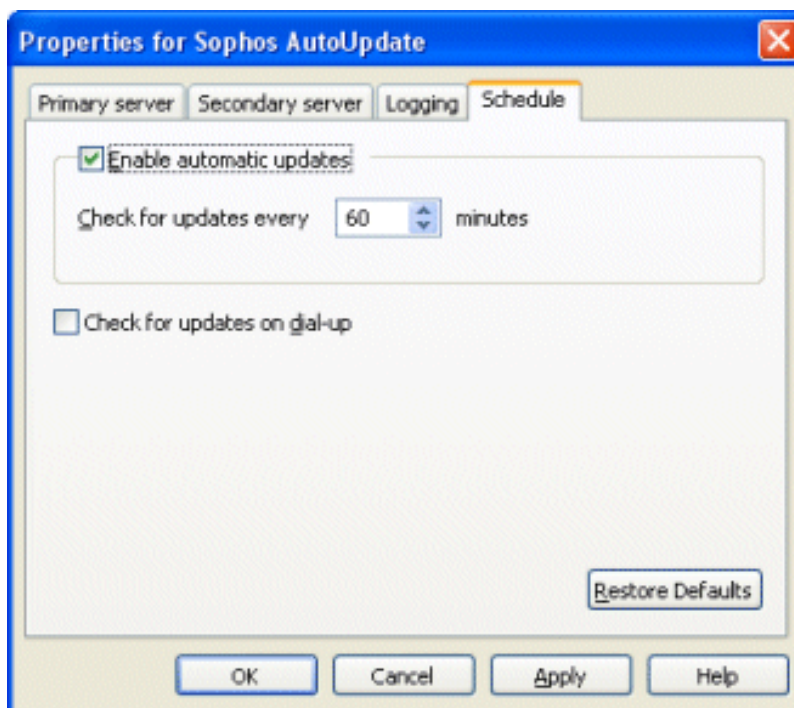
You can specify when or how often Sophos Anti-Virus updates itself.

i The central console, if any, that administers Sophos Anti-Virus on workstations may override changes made here. To avoid this, see the console help.

1. Locate the Sophos Anti-Virus icon in your system tray. Right-click on it and select **Configure**.



2. Click the **Schedule** tab.



If you update from the network, or via a broadband connection to the internet, select **Enable automatic updates**. Then enter the frequency (in minutes) with which Sophos Anti-Virus will check for updated software. The default is 60 minutes.

i If the updates are downloaded directly from Sophos, you cannot update more frequently than every 60 minutes.

If you update via a dial-up connection to the internet, select **Check for updates on dial-up**. Sophos Anti-Virus will attempt to update whenever you connect to the internet.

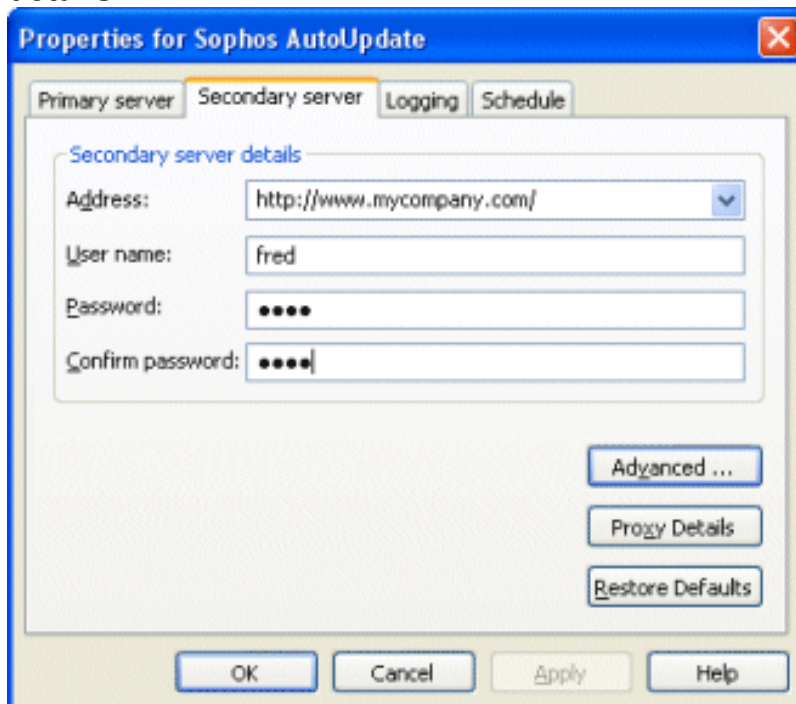
Updating via a proxy

If Sophos Anti-Virus fetches updates via the internet, you must enter details of any proxy server that you use to connect to the internet.

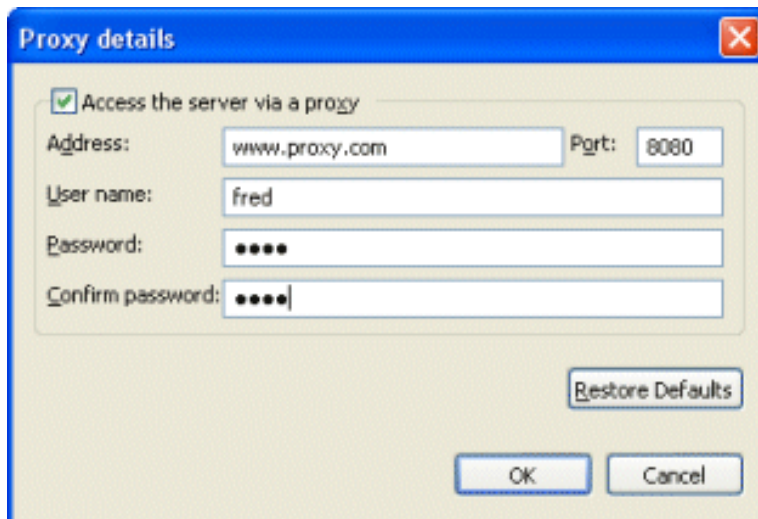
1. Locate the Sophos Anti-Virus icon in your system tray. Right-click it and select **Configure**.



2. Click the **Primary server** tab or the **Secondary server** tab as required. Ensure that all the details have been correctly entered. Then click **Proxy details**.



3. In the **Proxy details** dialog box, select **Access the server via a proxy**. Then enter the proxy server **Address** and **Port** number. Enter a **User name** and **Password** that give access to the proxy server. If the user name needs to be qualified to indicate the domain, use the form domain\username.



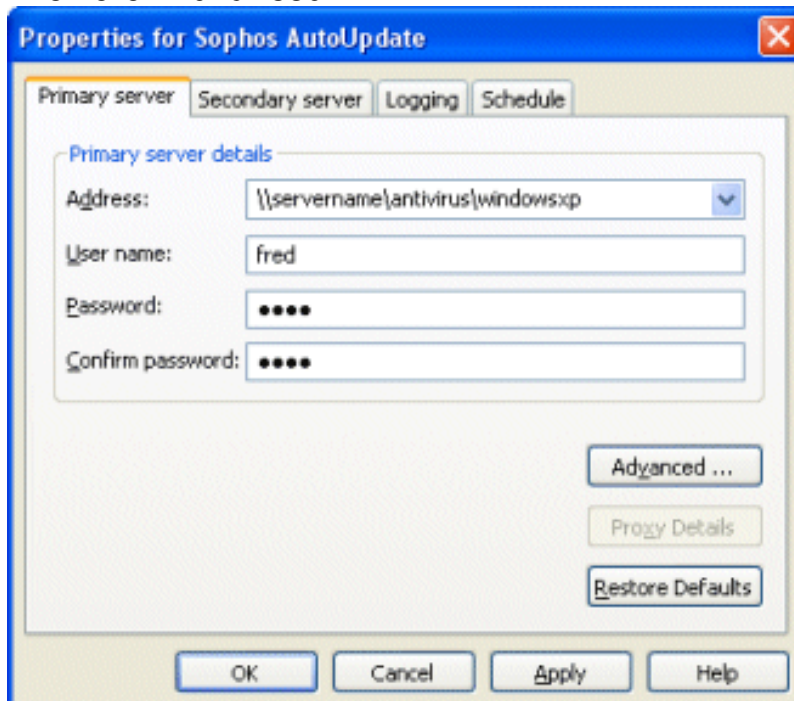
Limiting the bandwidth used

You can limit the bandwidth used for updating. This prevents Sophos Anti-Virus from using all your bandwidth when you need it for other purposes, e.g. downloading your email.

1. Locate the Sophos Anti-Virus icon in the system tray. Right-click it and select **Configure**.

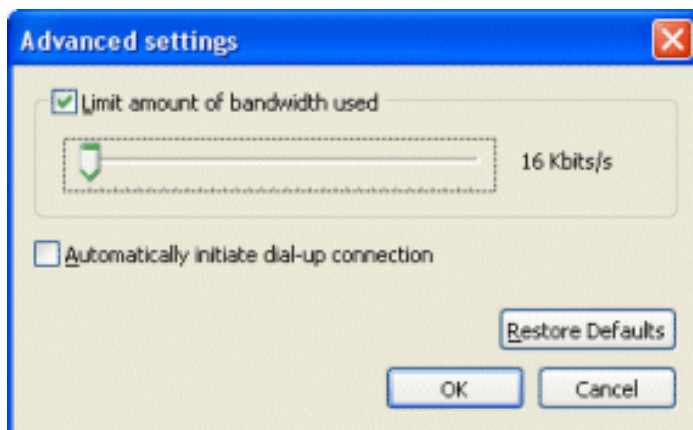


2. Click the **Primary server** tab or the **Secondary server** tab as required. Then click **Advanced**.



3. In the **Advanced settings** dialog box, select **Limit amount of bandwidth used** and use the slider control to specify the bandwidth in Kbits/second. If

you specify more bandwidth than the computer has available, Sophos Anti-Virus uses all that is available.



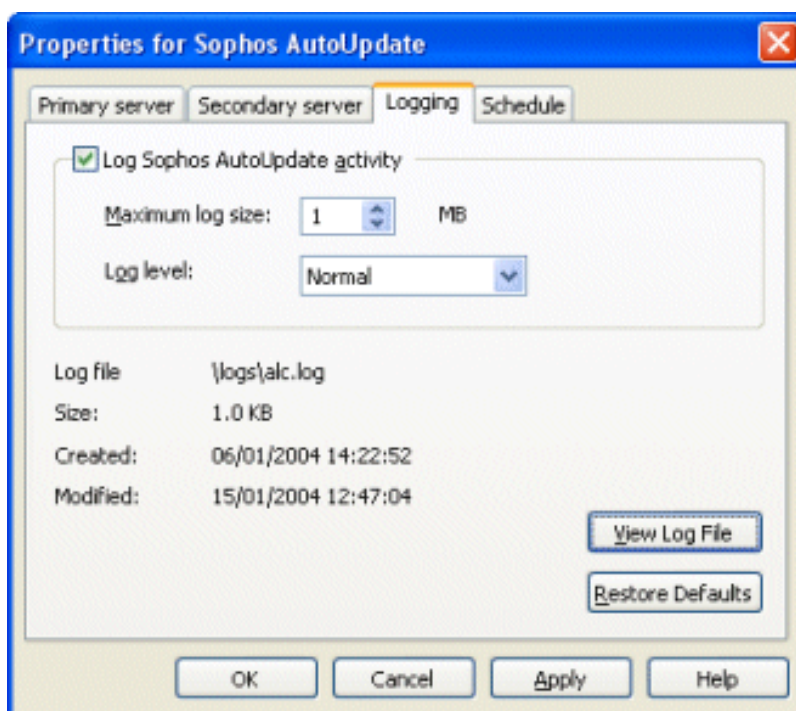
Logging updates

You can configure Sophos Anti-Virus to record updating activity in a log file.

1. Locate the Sophos Anti-Virus icon in your system tray. Right-click and select **Configure**.



2. Click the **Logging** tab. Ensure that **Log Sophos AutoUpdate activity** is selected. Then set other options as described below. When you want to open the log, click **View Log File**.



Maximum log size

Specify a maximum size for the log in MB.

Log level

You can select **Normal** or **Verbose** logging. Verbose logging provides information on many more activities than usual, so the log will grow faster. Use this setting only when problems occur.

Troubleshooting

This section provides answers to some common problems that you may encounter when using Sophos Anti-Virus:

- Updating fails
- Scanning runs slowly
- Scheduled scans do not run (95/98/Me)
- Virus not disinfected
- Virus fragment reported
- Sophos Anti-Virus reports errors.

If your problem is not described here, refer to the Sophos website www.sophos.com which includes a knowledgebase, virus analyses and technical articles.

If your problem is not described on the website, contact Sophos technical support.

Updating fails

If updating fails, a white cross is superimposed on the Sophos Anti-Virus icon in the system tray.

To find out more about an update failure, look at the update log. Right-click on the Sophos Anti-Virus icon and select **Configure**. Then open the **Logging** tabbed page and click **View Log File**.

The sections below explain why updating may fail, and how you can change the settings to correct the problem.



You need Administrator rights to change the updating settings.

Sophos Anti-Virus contacts the wrong source for updates

1. Right-click on the Sophos Anti-Virus icon and select **Configure**.
2. Click the **Primary server** tab. Check that the address and account details are those supplied by your administrator.

Sophos Anti-Virus cannot use your proxy server

If your copy of Sophos Anti-Virus updates itself via the internet, you must ensure that it can use your proxy server (if there is one).

1. Right-click on the Sophos Anti-Virus icon and select **Configure**.
2. Click the **Primary server** tab. Then click **Proxy**.

3. In the **Proxy details** dialog box, enter the proxy server address and port number, and the account details.

Automatic updating is not correctly scheduled

1. Right-click on the Sophos Anti-Virus icon and select **Configure**.
2. Click the **Schedule** tab. If your computer is networked, or if you update via a broadband internet connection, select **Enable automatic updates** and enter the frequency of updating. If you update via a dial-up connection, select **Check on dial-up**.

The source for updates is not being maintained

Your company may have moved the directory (on the network or on a web server) from which you should update. Alternatively, they may not be maintaining the directory. If you think this may be the case, contact your network administrator.

Scanning runs slowly

Immediate or scheduled scans may run slowly for the following reasons.

Extensive scanning enabled

By default, Sophos Anti-Virus scans only the parts of files that are likely to contain viruses. If you set scanning to **Extensive**, Sophos Anti-Virus scans every part of every file and takes significantly longer to carry out a scan.



Extensive scanning should be enabled only on advice from Sophos technical support.

Checking all files

By default, Sophos Anti-Virus checks only files that are defined as executables. If it is configured to check all files, the process takes longer. See the section on changing items for immediate scanning, or for scheduled scanning.

Network drives selected

Network drives can be much larger than local hard disks and so take significantly longer to scan. Most network interfaces provide much slower access than the local hard disk, which can further slow down the scan. Scan locally where possible.

Progress bar displayed

If the progress bar is displayed, Sophos Anti-Virus must count all items it will scan. This can take several minutes on large network drives. To enable or disable the progress bar, click **Progress bar** on the **View** menu.

Archive scanning enabled

By default, Sophos Anti-Virus does not scan inside archives. If you select **Scan inside archive files**, scanning may take longer. See Changing scanning options.

Scheduled scans do not run (95/98/Me)

In Sophos Anti-Virus for Windows 95/98/Me scheduled scans only run if the computer is switched on and the **Sophos Anti-Virus** window is open.

You can configure Sophos Anti-Virus to run scheduled scans when the **Sophos Anti-Virus** window is not open using AT.INI. This is described in the appendix of the *Sophos Anti-Virus DOS/Windows 3.1x user manual*, available on the Sophos website.

Virus not disinfected

If Sophos Anti-Virus has not attempted to disinfect a virus ("No action taken"), check that automatic disinfection has been enabled.

If Sophos Anti-Virus could not disinfect the virus ("Disinfection failed"), it may be that it cannot disinfect that type of virus.

You should also check the following:

- If dealing with a disk or removeable media, make sure that it is not write-protected.
- If dealing with files on an NTFS volume (Windows NT), make sure that it is not write-protected.

Sophos Anti-Virus will not disinfect a virus fragment because it has not found an exact virus match.

Virus fragment reported

If a virus fragment is reported, contact Sophos technical support for advice.

The report of a virus fragment indicates that part of a file matches part of a virus. There are three possible causes:

Variant of a known virus

Many new viruses are based on existing ones, so that code fragments typical of a known virus may appear in files infected with a new one. If a virus fragment is reported, it is possible that Sophos Anti-Virus has detected a new virus, which could become active.

Corrupted virus

Many viruses contain bugs in their replication routines that cause them to infect target files incorrectly. An inactive portion of the virus (possibly a substantial part) may appear within the host file, and this is detected by Sophos Anti-Virus. A corrupted virus cannot spread.

Database containing a virus

When running a full scan, Sophos Anti-Virus may report that there is a virus fragment in a database file.

Sophos Anti-Virus reports errors

The following error messages can appear in the **Sophos Anti-Virus** window, in the on-screen log.



In the descriptions below, text in square brackets indicates information that varies.

Error: InterCheck report:

[Message]

At [time]

User [user]

Node [network address]

This is an error reported by on-access scanning. The description of the error is contained in the [message].

Error: Could not open [filename]

The file called [filename] was on the list of files to be scanned, but could not be opened for examination. Check that the file is not in use or already open.

Error: Could not read [filename]

The file called [filename] was on the list of files to be scanned, but could not be read. This might indicate the file or disk is corrupt.

Error: Sector size of drive [drive] is too large

Sophos Anti-Virus currently only scans disk sectors of 2 KB or less in size. It is highly unlikely that your computer will ever contain sectors larger than this.

Error: Could not open report file [filename/folder]

The filename and folder of the report file are specified on the **Report** tabbed page of the **Immediate Scanning Configuration** or **Scheduled Job Configuration** dialog box (see Configuring reports). Sophos Anti-Virus cannot open the report file if its filename is invalid, or it doesn't have sufficient access rights to the folder. On Windows NT, note that the report file is written as the current user for immediate scans and as the Sophos Anti-Virus service user for scheduled scans.

**Error: Log file [filename] could not be opened.
Log data will not be saved.**

The location of the log file is specified in the **Log Folder** dialog box (see Setting the log folder). Sophos Anti-Virus cannot open the log file if it does not have sufficient access rights to the file or folder. On Windows NT, note that the log file is written as the Sophos Anti-Virus service user and not the current user.

Error: Could not notify [user]

The [user] is on the notification list but cannot be notified. This may be because the [user] is no longer on the list of recognised Microsoft Exchange users, or because a profile that requires the user to enter a password was used.

Error: Could not initialize mail system

Microsoft Mail may not be set up correctly (e.g. if the MAPI mail interface is not installed correctly).

Error: Could not login to mail system

If Sophos Anti-Virus cannot log in to the mail system, the profile name may be invalid.

Error: Could not allocate memory for [filename/folder]

If the report file is too big, Sophos Anti-Virus cannot load it into memory to send it to the users on the notification list. The report file can become very large if it is configured to list every file it examines (see Configuring reports).

Technical support

For technical support information visit

www.sophos.com/support

If you contact technical support, provide as much information as possible, including Sophos software version number(s), operating system(s) and patch level(s), and the exact text of any error messages.

Copyright © 2004 by Sophos Plc

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the licence terms or you otherwise have the prior permission in writing of the copyright owner.

Any name should be assumed to be a trademark unless stated otherwise.
InterCheck and *Sophos* are registered trademarks of Sophos Plc.